FedNow Commentary—BetterBuyDesign

Abstract:
Steve Mott, Principal at payments consultancy BetterBuyDesign, LLC, fully supports FedNow and participation of the Federal Reserve as an operator in the emerging faster payments ecosystem. The Fed's participation is essential for establishing a foundation for innovative real-time payment and funds movement through both its real-time settlement architecture and its availability to provide a competitive service platform that manifests interoperability, security and efficiency among RTP interconnections. It is vital that FedNow offer true and sustainable security sufficient to support irrevocable transactions when necessary and appropriate, as well as a 'plug-and-play' type of environment for applications from both banks and non-banks. To that end, the attached commentary focuses on 1) the ministrations and recommendations of the Standards Assessment Team (SAT) of the Secure Payments Task Force; and 2) a historical perspective on how Australia went about developing and fielding its New Payments Platform (NPP)—a model for the Fed to consider on how to craft FedNow to optimally support innovative applications from all parties. Contact: Stevemottusa@gmail.com or 203-5360588.

A. Standards and Security in the Era of Faster Payments

The new and emerging security threats for real-time payments has occupied a growing portion of the conversation on how faster payments systems ought to go about delivering a level of security proportional to and appropriate for the vast array of payments use cases that potential users are clamoring for—especially from FedNow. The Effectiveness Criteria contained 11 components of security, but all 16 proposers addressed most of them only at a high level (e.g., 'employ a high level of encryption'…'based on industry standards'). The problem is, industry standards for secure payments in an RTP world have not been developed yet (although a number of groups have begun work on them.

The sections that follow regarding security imperatives for FedNow were overall originally were developed by the SAT team working under the Secure Payments Task Force but ultimately produced and reviewed only internally with the Fed team responsible for this work group. There were other deliverables of the SAT group that dealt with amounts and sources of fraud, as well as assessment of solutions—including specific projects the Task Force (or some other entity) might pursue to wrestle the fraud issues—which the card systems in the payments industry tend to be reluctant to discuss openly (these networks and big banks produce nearly half the world's card fraud on only a quarter of the volume). Discussion of these deliverables were resisted, including with legal threats, by one bank card network and one banking association, during the course of SPTF/SAT work efforts.

Thus, it is incumbent on the Fed to separate the perspective and interests of the card systems from the rest of the payments ecosystem, and pursue FedNow and related activities with an

open, realistic appraisal of security requirements, threats, and options for making FedNow a more reliable, efficient and secure payment option than existing payment services.

A. SAT Security Report *(Partial)*

Standards are published documents that establish specifications and procedures designed to ensure the reliability of the materials, products, methods, and/or services people use every day. Standards address a range of issues, including but not limited to various protocols that help ensure product functionality and compatibility, facilitate interoperability, and support consumer safety and public health. Imagine life without standards for security and interoperability of the electrical grid, public water supply, highways, and communications. Payments should be no different.

Standards form the fundamental building blocks for product development by establishing consistent protocols that can be universally understood and adopted. This helps fuel compatibility and interoperability, simplifies and drives development of new products, and speeds time-to-market. Standards also make it easier to understand and compare competing products. As standards are globally adopted and applied in many markets, they also stimulate international trade.

It is only through the use of standards that the requirements of interconnectivity and interoperability can be assured. It is only through the application of standards that the credibility of new products and new markets can be verified.

In order to support the Federal Reserve's SPTF workgroups in their consideration of changes needed in the U.S. payments system, a group of security and standards specialists were recruited to identify gaps that available (or prospective) standards could address. This Standards Assessment Team (SAT) canvassed fraud threats, identified impediments to adopting better security, reviewed new technology options for safer transacting, and surveyed standards initiatives for use as a reference by the workgroups. SAT found that fraud was rampant in some existing payment streams (but unknown in others), owing mainly to the inability of the industry to collaborate effectively on adoption of eight essential security principles and controls:

1. No account credentials in the clear
2. All data protected with suitable (open) encryption standards
3. Identification/verification (ID&V) of parties
4. Assurances/ levels available to measure risk
5. Account and ID credentials encrypted and rendered in secure objects
6. Robust access controls and interconnectivity
7. Data integrity checking and verification
8. Behavioral monitoring checks and verification
9. Standardized management and oversight of 3rd party service providers

These security controls apply to some or all of the payment methods that PIM, I-S and DP are analyzing and will be described in more detail later in this report.

Most of these security principles and controls have been developed by a broad consensus of industry participants working in accredited standards organizations (such as NIST and ANSI ASC X.9), are widely used by organization across the globe, and frequently considered by regulatory agencies in the public sector (and used by Federal agencies).

On the other hand, the nation's legacy payment streams—predominantly payment cards, electronic checks (ACH), wire transfers (e.g., FedWire) and paper checks—are primarily governed by proprietary organizations representing the main providers of the stream (e.g., EMVCo for card payments interoperability (which impacts security), or rule-making bodies operating on behalf of financial institutions (FIs), such as NACHA for the ACH, EPN/TCH for wire transfers, ECCHO for checks. This group, which broadly comes under the aegis of the Federal Reserve, has built a very large and functional payments system, but also one that is experiencing growing fraud and escalating cyber-attacks.

The fearsome specter of cyber-attacks has unified the government, regulators, and some FIs, creating a good role model for leveraging recent standards work performed in the public sector (e.g., NIST's Cyber Security Framework) for adoption in the private sector. While this is a useful precedent for public-private sector collaboration to combat electronic attacks that lead to fraud, compromises of confidential information, and threats to the national infrastructure, cooperation for addressing and eliminating the *sources and causes* of fraud between the payments industry and the federal government sector—especially embracing and leveraging existing security standards—continues to be lacking.

Such a deficiency has led to a growing view that the U.S. is unconstructively fraud-prone (e.g., the country produces 23% of the world's card payments but nearly 43% of its fraud[1]). This situation, and related payment risk and operational inefficiencies owing to the lengthening 'tether' to physical processes (such as 15 billion paper checks with account credentials fully exposed still floating through the system), has led to serious questions about the country's ability to competitively support the inexorable movement to fast-moving digital transactions and the conduct of economic value exchanges. Moreover, a number of examples of this industry ineffectiveness surfaced in SAT's discussions and review of the current situation confronting the payments system.[2]

While clearly there are gaps in what users of the payment system expect and need, SAT's interactions with some members of the SPTF workgroups suggest that there might be some disagreement about what those gaps are, as well as some reluctance to discuss how severe the gaps might be and how to address them.

To that end, SAT endeavored to provide a fact-based assessment of the current environment, using the payment type and use case analysis theme it helped develop for two of the workgroups to ensure issues with existing payments were surfaced for review, and to illustrate the challenges for security with digital (real-time) payments.

Where actual standards *are available and do apply* (such as PIN-debit), those are identified. But the predominant array of standards that would be crucial for securing existing and new digital payment types—including faster payments models—remain in the public (federal government) domain—largely unutilized by the payment networks in the private-sector.

[1] Nilson Report, Issue #1096, October 2016 (adjusted for consistency with 2015 report)
[2] Summaries of these findings and perspectives follow in subsequent sections of this report. Detailed assessments are provided in the Appendices.

SAT also suggested one or more collaborative projects between legacy providers and the broader, evolving payments ecosystem for each payment type use case within the PIM, I-S, and DP workgroups. These suggestions for collaborative research were aimed both at resolving some conflicting views (where possible) by coalescing the full data needed for objective assessments, and at setting the stage for more concrete initiatives (pilot tests, creating new standards where needed, etc.) that 'move the needle forward' on improvements in security in the near-term (1-3 years).

For the longer term (3-5 years), SAT deliberated on the need for and efficacy of the nine fundamental principles/controls referred to above. The team also described several supporting work products as a 'stalking horse' for a holistic set of solutions to fortify the security of the payments system in a sustainable fashion. These solution components identify existing or recommended standards to underlie the potential changes in the payments system that SAT believes are necessary.

SAT presented itself as a resource for the SPTF workgroups, and designed some of its work products as a sustaining resource for any follow-on version of the SPTF (or the Fed) to use in continuing and comprehensive assessment of gaps that can be addressed by existing or proposed standards. All of these work products are provided in summary form in the report, with examples in the Appendices.

Figure 11. Security Controls Summary

Security Controls Summary							
Security Controls/Principles	Manifestation in Long-Term Solution	PIM	Info-Sharing	DP	Industry Certification/ Integration/ Testing Role Required	Central Authority Operating Role	Central Authority Activities & Responsibilities Expected
No account credentials in-the-clear	Multitude of credentials, available by choice and payment authorization requirements, all encrypted with vetted open standards	X		X	X	(An operator of national payment hub with full participant choice)	Provide an alternative (default) network hub/integration platform that prevents exposed account credentials, enables flexibility in participation, and promotes secure access and liability assignment
All data protected with suitable (open) encryption standards	Multitude of cryptos supported, using open, non-proprietary standards that support global interoperability	X	X	X	X	X	Convene college of standards bodies and payments ecosystem to set bar for adequate encryption; facilitate interoperability and testing; certify providers and participants; manage industry key structures and root(s)
Identification/verification of parties	Standard, sharable identity proofing and management, with multiple authentication options and factors; validation and verification of participants, universal user addressing conventions and real-time checking	X	X (for access)		X	(Set standards and provide APIs for interoperability)	Define baseline for acceptable multi-factor configurations for use, including risk elements and parameters, and metrics for monitoring; create and manage industry directories/ addressing tables, good/bad actor lists, etc.
Assurances/levels available to measure risk	Access to multiple assurances, pertaining to payments and risks, available to any size and type of participant	X	X		X	X	Coordinate availability and validation of assurance mechanisms (NIST, EMVCo, etc.); support robustness and accuracy over time
Account and ID credentials encrypted and rendered in secure objects	Embedded security permitting freely exchanged object throughout the end-to-end processing chain	X		X	X	(Set open standards/ updates)	Define acceptable embedded security protocols to xML and other object-oriented paradigms to protect data at its origin
Robust access controls and interconnectivity	Tiers of access validation and permission levels based on value/risk of payments and transfers, with fluid, complete and secure industry interconnectivity		X	X	X	X	Apply to FedWire first, encourage adoption in CHIPS, SWIFT, CHAPS, etc.; Support Constructive Key Management (CKM) under X9-69 and X.9-73
Data integrity checking and verification	Best practices/common basis for checking and reconciling data throughout processing cycle		X (Consistency)	X	X	X	Establish baseline for acceptable mechanisms for data checking, and cross-payment rules and standards for following them
Behavioral monitoring checks and verification	Includes secondary advice/alerts using anonomous sets of data for users and transactions	X		X	X	(Provide industry access)	Assist development to ensure appropriate levels of privacy and access control are implemented and participants are vetted
Standardized management and oversight of third party service providers/suppliers	Coordinate increased management of the supply chian risk by vetting third party providers with share assessments and vetting/monitoring procedures	X	X	X	X	X	Define security requirements, qualifications and monitoring procedures for providers to serve regulated financial institutions at each stage of the payment processing cycle

At a high level, these controls together constitute a 'distributed security framework' (Figure 12) that can reside on an integrated platform (or 'hub', as Australia terms its New Payments Platform (NPP), which will be available online in summer of 2017)[3]. By interconnecting all the security controls and utilities described above, such a platform can provide many innovations in payments, including:

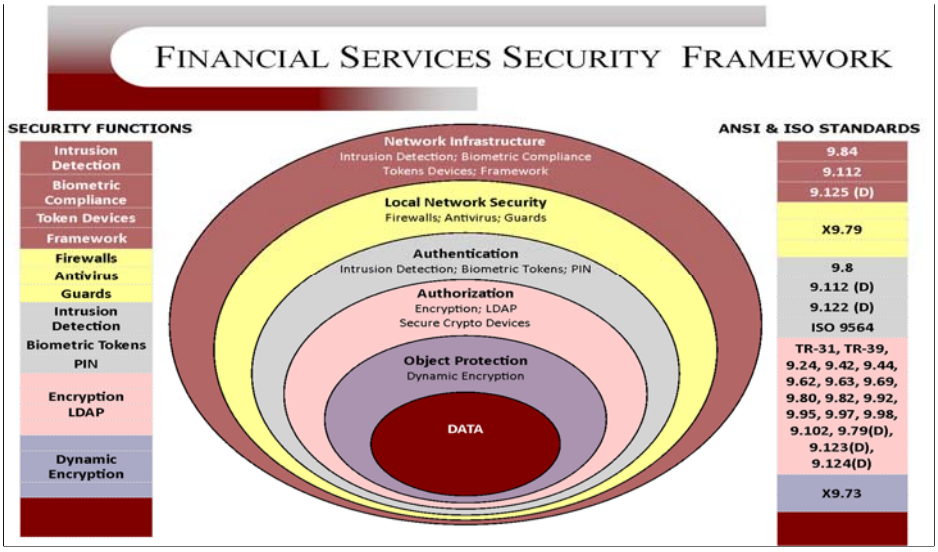
- Supports many different authentication and account credentials—enabling massive connectivity and nurturing the security solutions industry to enter the commercial sector and grow into a critical role
- Protects all data with open, vetted and certified forms of standards—obviating much of the threat of cyber-attacks and data compromises, while nurturing necessary advances in cryptography
- Provides tiered and varied levels of identity proofing and management selectable by participants—facilitating adoption and contouring of identifying and verifying payments and

[3] Please see Appendix K—Australia's New Payments Platform (NPP) *[Provided in Original Form, in Part, following this section]*

participants based on attributes, and supporting address directories, green-lists, bad-actor lists and related services

- Accesses emerging and varied assurance levels and their provisions—helping users access industry- and payment type-based risk assessments
- Renders all payment and ID credentials in protected object form—enabling anonymous (and protected) surrogates for payment credentials to pass securely throughout the digital payment system
- Standardizes access controls, and enables interconnectivity to vetted new payment services—securing the endpoints of connecting networks and making available "brokered" competition for payments that cannot operate on existing payment rails, assigning liability levels based on risk and cost so that payment can be guaranteed (or not), and interconnecting with payment systems around the world for choice in service parameters and delivery.
- Establishes standards and certifies protocols for data integrity checking and verification—ensuring error reduction, spotting payment inconsistencies, and preserving continuity of key data (e.g., amounts) as a risk management tool
- Provides foundation for developing user profiles with behavioral attributes—establishing a capability to risk-assess participants based on how they have used the platform

Figure 12 – Financial Services Security Framework (from TecSec)[4]



These controls are designed to interoperate in an open, global, interconnectivity platform available from one (or more) Central Authority(ies)—giving FIs, retailers, third-party providers and consumer/business users that are seeking digital payment options that might not otherwise be available in the emerging marketplace. Moreover, these controls can operate under open, non-proprietary global standards—accredited standards developed by the industry, but thus far adopted almost exclusively by the Federal government—not the payments industry[5]. 'Industry' ownership of security protocols and rules for their

[4] TecSec is an Annapolis firm that specializes in comprehensive security solutions, and is active in ANCI ASCx.9 standards and industry based Quantum Computing assessments

[5] A number of 'decrees' from the White House and Administration agencies [e.g., FFIEC guidelines for multi-factor authentication (2005, with updates), Department of Homeland Security-Directive 12 establishing rules for identification (2004), Whitehouse mandate for the use of PINs (2015)]

use offers the potential to relieve the legal and regulatory pressures due to monolithic rule-making by FIs and networks, and the ability of the networks to impose investments in security with little or no ROI.

Importantly, implementation of the controls will in many instances require a facilitating and trusted Central Authority to organize, operate and standardize this deployment[6]. Australia (and other countries) concluded that the industry itself would not be capable of creating open, competitive, and efficient digital payments in the timeframe needed to stem fraud and enable applications. A trusted—and objective—Central Authority (such as the Fed) would also establish and adjudicate root keys and key management systems necessary to make such a security solution operate.

These controls also address most of the anticipated outcomes and recommendations of the SPTF workgroups.

What Problems the Nine Controls Address

The nine principles/controls, in combination, address the major elements of a fully manifested new paradigm in digital security that protects the nation and the economy with a highly secure, efficient and flexible new infrastructure. But each of the nine also faces significant hurdles to adoption that must be resolved (Figure 13).

Figure 13. Security Principles Fixes and Impediments to Adoption

Security Principles/ Controls	What They Fix	Impediments to Adoption
No account credentials in the clear	Eliminates compromise risk in-transit and at-rest, as well as targets of cyber attacks	Cards and checks depend on account data for routing and processing
All data protected with encryption	In addition to account data, encryption of PII and related data prevents account takeover through social engineering	Massive amounts of PII (e.g., Social Security Numbers) are already exposed, and used for account identification
Identification/ verification of all parties	Acceptable standards for ID&V with digital objects and multiple-factors ensures origin of and access to accounts are valid and trusted; directories and 'green-lists' reduce errors and alert users to risks	Most payment accounts are held by regulated FIs using legacy, physical-form IDs and credential; changes to auditable alternatives will be large—necessitating industry utilities/services to reduce costs
Assurances and levels available to measure risk	Access to a choice of emerging assurances provide a basis for digital trust	Trust verification services are new and not yet tested at scale; real-time use requires industry utility to offer connected access
Account and ID credentials encrypted and	Digital, mobile and real-time networks globally require object formats (e.g., XML) for synchronized use end-to-end in transaction chain	Global standards will need to be agreed upon and legacy payment systems will have adapt to object creation, processing and storage

[6] Appendix M presents a TecSec white paper from SAT members Jay Wack and Ed Scheidt that describes in detail how these protections can be deployed using nearly completely open/non-proprietary accredited standards that accommodate a free-market for security tools and capabilities that meet the Central Authority's bars for acceptable levels of effectiveness.

rendered in object form		
Robust access controls and interconnectivity	Network encryption is augmented with stronger, standardized access controls configurable to specific user levels and risks	Industry inertia to be lax about access must be overcome by network rules, monitoring, and enforcement
Data integrity checking and verification	Preservation of key data items such as transaction amounts are critical to real-time risk management and settlement	Industry move to tokenization and chip without data integrity checking is already underway and expending resources
Behavioral monitoring checks and verification	Digital and mobile data sets and usage patterns complement real-time risk management and feed attributes-based identities	Privacy concerns will require protections with user objects/attributes confined to transaction histories
Standardized management and oversight of third party service providers/suppliers	Interdependencies of payment partners along the supply-chain make it mandatory to ensure there are no weak links anywhere in sequences of providers	Lack of supervisory jurisdiction and control historically creates an uphill struggle to require 100% conformance with standards that evolve continually; enabling legislation might be required

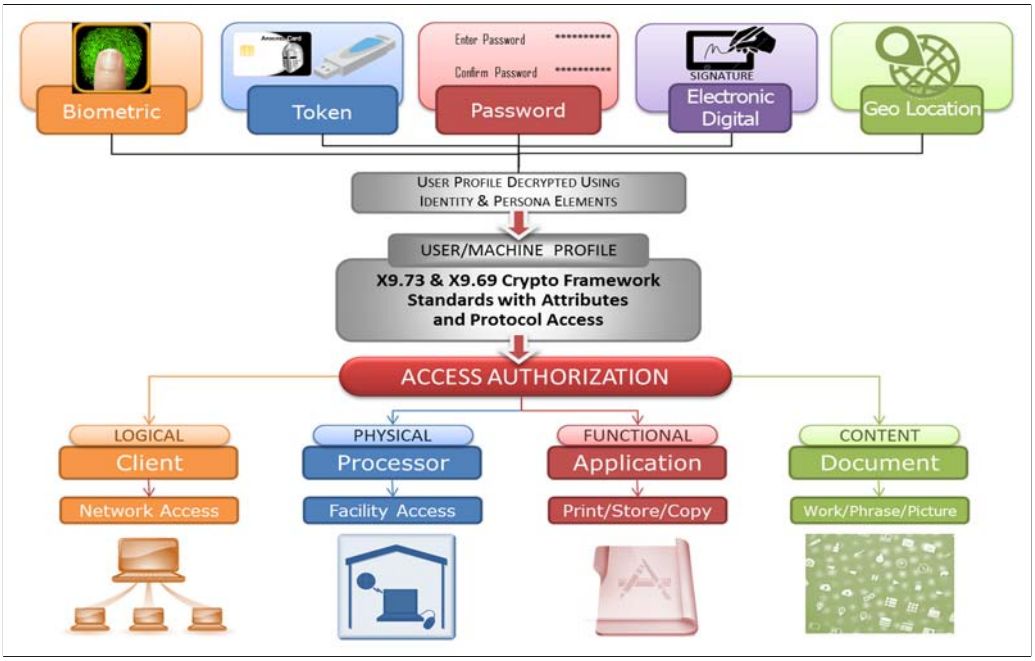
How the Solution Works[7]

Identities can be invoked with an increasing array of technologies. Passwords have existed since the dawn of electronic access (i.e., corporate facilities, then Internet websites). Electronic/digital signatures and certificates have also existed in corporate transaction environments. Tokens, which have been used in electronic environments for years are now moving to payment cards, and perhaps to all bank-oriented payments in the foreseeable future. Mobile payments and networks now provide geo-location data, and biometrics appears to be emerging with the newly announced 3-Domain Secure (3DS v2.0), which the network brands plan to apply to the ecommerce domain.

The expectation is that the array of technologies and methods for establishing identity and persona elements can and should accommodated, provided they are vetted to meet minimum encryption standards. Rendered in secure objects, these identifiers can all be assembled and arranged into user profiles (associated with machine profiles), with various forms of access managed by cryptographic framework standards such as X9.73 and X9.69—nationally recognized open standards (Figure 14).

Figure 14. User/Machine Profiles

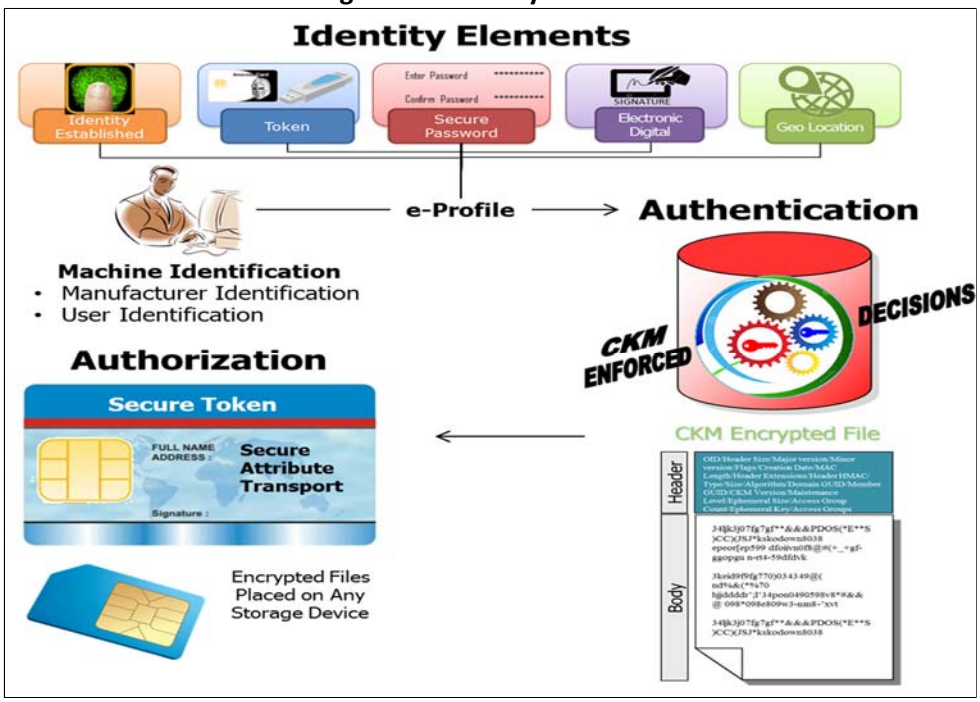
[7] A more detailed explanation of this summary description and other element of the solution are provided in Appendix M: TecSec Paper on Identity, Authentication, and Data Protection. (Not provided here)



Source: TecSec

Operationally, user identity elements in "e-Profiles" and "Machine Identification" elements can be authenticated in a universal fashion—within the integration platform—provided that these credentials are encrypted and recognized via a common cryptographic environment (Figure 15).

Figure 15. Identity Elements



Source: TecSec

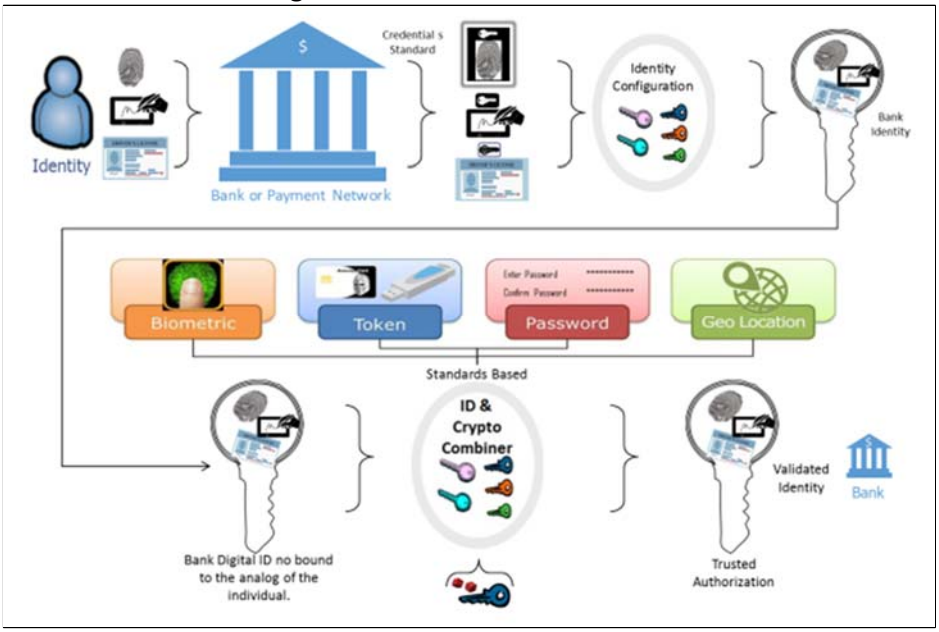
NIST's Constructive Key Management ("CKM") as defined in ANSI X9.69 and X.9.73 provides a common crypto key root and dynamic key management, and offers a system that relies on the assignment of

subject attributes to subjects and object attributes to objects, and the development of policy that describes the access rules for each object. Each object within the system must be tagged or assigned specific object attributes that describe the object. Users can also transport their profiles and attributes on secure tokens and storage devices, ensuring transportability.

During the process, users would engage in this architecture as follows (Figure 16):

1. Establish identity (in physical and other forms) at a participating FI
2. The FI participates in a bank or payment network that can connect to the integration platform, and provides the protected credentials
3. Those credentials can be mix-and-matched for particular identity configurations and requirements, and then transported via the bank digital identity to the security infrastructure of the integration platform ("ID and Crypto Combiner").
4. The integration platform validates the credentials with standards-based processes appropriate to the user, bank and transaction
5. The result is provision of trusted authorization, validating the identity to the bank, which is relying on the platform to provide these services (if not available through private-sector networks)

Figure 16. Solution Process Flow



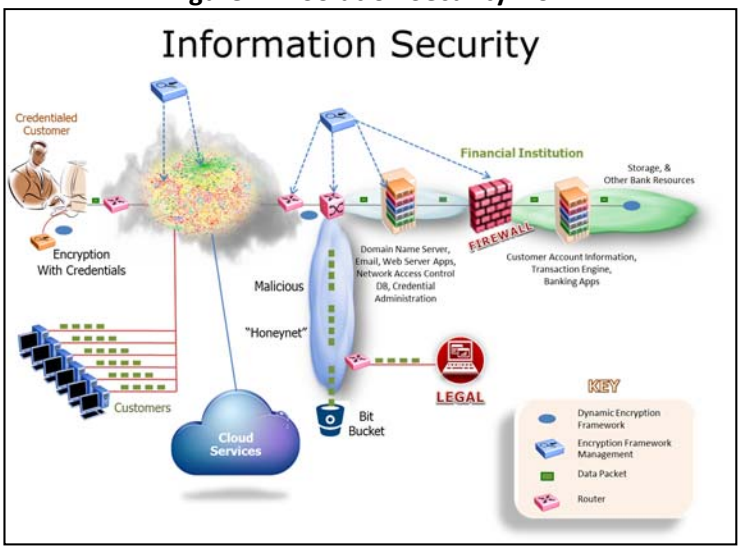
Source: TecSec

Due to the nature of the cryptographic operations and management responsibilities, a "Central Authority" is contemplated for general use—on a default basis to address several requirements:

- To interconnect multiple networks for ubiquitous access to thousands of banks and credit unions—in the U.S. and beyond
- To provision of a default settlement network that all parties and networks could use
- To provision of a full array of user choices—should those preferences not be available from private sector networks and services
- To provide the ability to interconnect globally, without the requirement for different countries to operate on a single cryptographic root key and process.

The Central Authority (possibly the Federal Reserve) would operate the integration platform as an industry utility, vetting security components, sorting through identity and authentication options, and interconnecting the world. As a centralized, consolidating platform, the Central Authority can direct problem transactions to a "honeynet" for further inquiries, investigations, and resolution (Figure 17).

Figure 17. Solution Security Flow



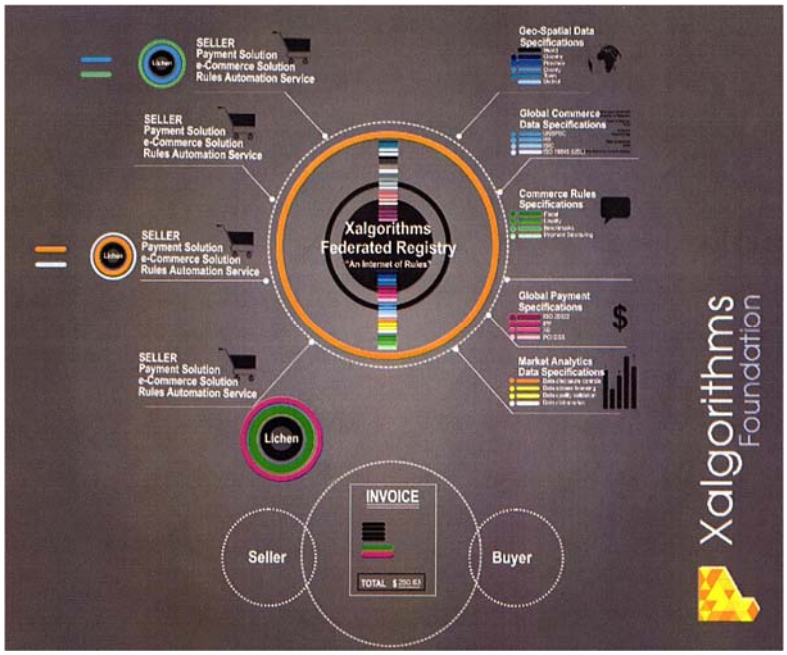
Source: TecSec

Accommodating Other Value-Added Services

Such an information security platform can and should also be used to interconnect with other value-added services that enhance the security, efficiency and usability of digital payments.

For example, the e-Algorithms' 'payment system browser' approach enables a user to search among payment service providers' rules, rates and regulatory provenance to select—in real-time—an optimizing (or default) choice for a payment transaction coming into the platform. Such a capability could help corporate users figure out how to legally and securely move funds under difficult or challenging circumstances (Figure 18).

Figure 18. Payment System 'Browser'



Source: eAlgorithms

Such a value-added service could also be part of an adjacent, interconnected platform (deploying SaaS) for enabling smaller FIs and businesses to connect with the real-time payment networks, or to utilize emerging ISO 20022 services that are too complex and expensive to deploy independently (i.e., in a Platform-as-a-Service mode). This is similar to the SaaS business model that the Fed, as an operator, already provides smaller FIs with for ACH and wire transfers.

Similarly, encryption can be provided on a 'Cryptography-as-a Service' mode with today's technology. And the needed interconnection of all these networks and services could be deployed by a Central Authority in an Infrastructure-as-a-Service' basis—replicating the Fed's existing platform configuration (i.e., IBM's Financial Transaction Manager).

Other payment registry services, including 'green-lists', 'bad actor' lists, IP/proxy server alerts, etc. can be developed and maintained by a Central Authority, and be housed on and accessed from this integrated platform. Ultimately, such an interconnecting platform can offer a virtual marketplace for a vast array of vetted certified security and payment service options to accommodate just about any transaction—and user—that needs a default service from a trusted, non-competitive entity.
In addition, this platform accommodates an ability to host, test, and validate just about any conceivable security technology, protocol, or device; successfully vetted pilots will channel the information and results consistently to the appropriate standards bodies in order to expedite availability to the marketplace.

The Central Authority can also make this technology available to other networks (subject to any operating license or IP considerations). It can also interface with the ITU, UNCITRAL and other groups around the world, Connected Cars, Smart Cities and the Internet of Things (IoT), all of which are working on secure transaction systems that don't necessarily need payment networks, and provide a test bed for proactive cyber security approaches and technologies (such as the 'cyber microscope' for monitoring transaction data bit-by-bit in-transit over open networks).

SAT members concur with the prevalent view in the SPTF that a Central Authority is needed to bring to the U.S. payments system all the improvements of security required for the digital transaction era. This challenge is not confined to supporting faster payments, but also to ensuring the integrity of the payment system itself.

Moreover, there are a multitude of examples of the dysfunction of the payments industry in reaching consensus on what to do, where, and when, and with what priority, and at whose expense? Without overt influence of a Central Authority, there is great skepticism that any meaningful progress will be made.

Industry Challenges with Faster Payments

Importantly, the Fed has been identified as a key participant (e.g., as a default settlement network, as a provider of participant directories, as a convening point for interoperation of these networks, etc.) to support most of the 19 proposed faster payment systems coming to market as identified and presented in the FPTF solicitation. These legacy challenges described in Figure 19 must be addressed with substantives changes in the status quo in order for faster payments systems to succeed.

Figure 19. Industry Challenges with Faster Payments

Challenge of Real-time Payments	Example of Industry Hurdle	Faster Payments Opportunity
1) Moving to near **real-time digital execution capabilities** at the technology's pace, rather than being gated by legacy system and risk management limitations with processing latencies built-in.	Execution of online check deposits and bill payments takes days (even 'expedited' fee-based payments), with no meaningful guarantees that result in unnecessary costs and user aggravation.	Options for real- or near real-time consummation of payments (or funding commitments) are now in development
2) Providing an **industry/ global 'sandbox' for** testing real-time transacting to facilitate and vet innovations in security approaches and technologies that often elude the industry.	With rare exceptions (e.g., PayPal in ecommerce), it has been difficult for innovators to break into the regulated financial services industry and reach a critical-mass level of acceptance	The ability to test and compare the capabilities of providers' products will provide FIs of all sizes a basis with which to qualify providers, and participate on viable terms with new services (e.g., ISO20022).
3) Getting the **public sector** with its interest in supporting *all* users of the payment system, and legacy providers with proprietary, **private sector** payment networks and services, to **collaborate on security initiatives** that are cost-effective and beneficial to all.	There are wide differences of opinion on the effectiveness of PCI and EMVCo requirements for mitigating data compromises; challenges to the purported benefits make users reluctant to deploy them, when they feel their resources could be better spent on better security (e.g., encryption).	Before new, alternative payment modes reach the payments mainstream, the entire ecosystem should holistically weigh in on ways to test the strength of security, and how industry standards for interoperability might be developed before critical-mass usage/vulnerability is reached.
4) **Convening a standing industry organization to assess and set best practices and**	While wire system operators continue to claim that the networks themselves were not	There is a burgeoning consensus that networks can only protect the endpoints of those networks if

prioritize fixes for better security; and to understand and provide input on the basis of costs and risks to encourage adoption of more secure digital payments; e.g., problems on wire transfer networks requiring consensus best practices for access controls.as opposed to letting users determine their own ways of interacting with digital networks	compromised, there was growing agreement that the 'end-points' of these systems suffered from inconsistent and ineffective user security practices—including inadequate access control, untimely resolutions of data integrity issues, etc.	data is protected with strong encryption and users are vetted. That means effective and different access controls, and more choices for what security is needed and used, as some faster payment systems are promising.
5) Encouraging **development of more flexible and differentiated marketplace options** for secure payments and security in digital venues and formats.	Network programs such as tokenization, 3DS online push, and discouragement of PIN use demonstrate the lack of adequately vetted and substantiated payment options available to users for more effective security.	Merchants, digital venues, and third party providers could appeal directly to consumers and small businesses to utilize those options; then the networks could compete on the relative value that they do or do not provide.
6) **Accommodating more user selections in the security services** they need and want, including creation of a foundation for hosting an open market for new types of transactions with more security, service and options (e.g., what options can execute a payment of *X*$ in *Y*hours in *Z*country at *W*fees.?)	Companies and consumers increasingly make cross-border payments and/or travel abroad, incurring high fees for wire transfers, foreign exchange conversion, problem resolution and other services—yet have very few service options to choose from. These limitations restrict and impair digital commerce, pushing users to alternative payments that might pose unacceptable risks.	Digital payment platforms can and should accommodate the full panoply of security protocols, measures, open standards and risk assurances and liability constructs available, provided they are certified at a suitable level. A Central Authority could validate and support new service options for security and interoperability
7) Facilitating market-making capabilities of the long-term solution to **foster a variety of liability allocations**, with chains of trust, including meaningful payment guarantees needed to improve digital commerce.	A multitude of parochial trust verification services are springing up around the world, but few interlink and interoperate, and almost none actually trust each other; liabilities, risks, and fees are assigned—not negotiated.	An integrated, facilitating industry platform that is capable of switching credentials, cryptos, assurance levels, transacting venues and global payment network rules can support an arrangement of assurance levels and liability tiers defined by optional trust frameworks
8) Finally, **coalescing and leveraging baseline, open standards** is essential to bringing the entire payments ecosystem—old and new—into alignment with security that has meaningful competition on marketing—not baseline security	Most U.S. payments are governed by proprietary *specifications* (e.g., payment cards by EMVCo, PCI, etc.) with nearly monolithic decision-making on rules, rates, and security requirements, or by banking industry organizations (e.g., ACH with NACHA, ACH/Wire with EPN/TCH), instead of open, non-proprietary standards.	New integrated digital networks can enable a wide variety of services, rules and rate options to match up with suitable security protocols and options, and provide interconnectivity via fluid access into and out of multiple such networks, interoperability as desired, and competition based

		on marketing value propositions —not common security

Industry Struggles in Achieving Consensus on Fraud (and Fixes)

In addition to the challenges that real-time payments pose for today's payments infrastructure and performance, there are fundamental examples that illustrate the issue over whether the payments industry *itself* is capable of making the necessary changes without some overt assistance from a Central Authority (Figure 20).

Figure 20. Security Gaps and Concerns by Use Case[8]

Use Cases	Perceived Gaps	Apparent Consequences	Possible Concerns
Signature Debit and Credit	Billions of account credentials remain broadly in-the-clear—even in EMV deployment (except for an encrypted CVV)	An estimated billion card credentials have been stolen in data breaches and cyber-attacks; a thriving black market 'backlog' exists.	Tokenization and other expedients (e.g., 3DS 2.0) might just be temporary 'patches'; mag-stripe and EMV card exposures are not addressed.
PIN-debit	PIN verification is widely viewed as one of the only current 'arrows in the nation's quiver' to reduce today's fraud, and is known to protect transaction data because the PIN data is encrypted using a global standard. But some consider it only a stop-gap because of its static identification and growing use of ATM skimmers.	Opportunities to secure more debit cards and even credit cards is discouraged by preferences of network brands to preserve signature-debit and credit and steer marketplace way from PIN.	Network brand support for alternatives to static PINs within three years (e.g., OTP, Dynamic pins, etc.) pushes industry to untested investments that could be better directed to encryption (or even full tokenization).
Prepaid	Open-loop prepaid could be secured along with regular credit and debit cards with encryption of credentials (and PINs in the interim); closed-loop prepaid could at least use PINs; both types need better KYC identification and access protections.	Successful hackers and thieves use prepaid card purchases to cash-out on their stolen credit and debit card credentials.	Desire of prepaid industry participants to avoid regulations (including consumer protections) forestalls need to secure this growing payment type (which is used disproportionately by the underbanked consumers.
P2P/Digital	New, fully digital payment types range from card-to-card to independent modes of monetization, which use some form of in-network or external protections, but under no	Hackers and thieves could migrate to digital payment modes when they discover protections might be weak in systems that utilize regulated FI accounts.	Credit-push—the preferred mode of monetization, is vulnerable to account takeover; debit-pull modes can result in typical fraud—but with funds absconded with faster

[8]The above examples of the payment industry's challenges with real-time payments and its struggles with achieving consensus on security and solutions are discussed in more detail in Appendix I. "Why the Industry Needs Help to Become Secure."

	common standards or verification methods (ID&V).		
ACH	ACH fraud based on lowered acceptable return rates, and increased measures to prevent account takeover and bogus origination (e.g., a bad actors list) appear to provide a stable foundation; faster settlement times—currently targeted to low-fraud use cases (e.g., expedited payroll)—could tax risk management in the future.	High dollar-volume transaction streams have a near-term capability using existing interconnections, formats, and conventions; future use cases could pose issues without standards-based tokenization and encryption.	Consideration of a move to more conventional tokenization (e.g., under the current plans of TCH) will be complicated by the 35+ year-old formats; opening up to broader sets of originators and higher-risk use cases should be assessed.
FedWire	Continuing cyber-attack threats and involvement in SWIFT exposure puts a premium on ensuring strong network encryption and user access controls.	As a likely default settlement network for multiple faster payments systems, FedWire will need to determine security of interconnections and broader use.	Users of multiple faster payment systems, which interconnect with the banking system via FedWire (and possibly other settlement networks) will need solid liability assessments.
Blockchain	Some industry collaborations suggest move to standards—especially for encryption and other security—but at present, none of these systems are trusted, and ledgers expose confidential data to dozens of unvetted partners.	This promising technology requires standard protection in order to get out of the pilot stage and fulfill its potential; identity proofing and management by a trusted 3rd party is required.	Ultimate need for some sort of confidentiality will likely require identity proofing and restrictions on access that some participants might resist.
ecommerce & Mobile	Online and mobile commerce are becoming magnets for fraud, especially with EMV deployment and data compromise, and have minimal protections (e.g., little use of PIN online, growing tokenization, inconsistent encryption; vast majority of consumer protections provided by merchants—not issuers or networks.	3DS v2.0 expands protections for little-used protocol, but gives inexperienced issuers ability to override 5% of merchant risk decisions, and issuers incentives to increase decline rates for transactions 'in the wild'	Network brands seek to control security for these fast-growing channels for transaction volume and issuer profitability; EMV does not apply but spurs threat; no standards for mobile security yet.
Check	Account credentials exposed on 15 billion pieces of paper defies electronification and continues to pose problems for businesses; high processing and fraud costs for all parties.	Exposure to high numbers of bank accounts could continue for decades, and attract thieves that might be repelled by securing other modes of access to DDA (e.g., debit cards).	Changing decades-old users and systems to ban processing of account credentials represents an expensive change, and might only be addressed by mandating an end-of-life date and/or making users pay the full costs.

Wallet	Extensive use of tokenization, fingerprint IDs, and other modes of protection appear helpful, but security of mobile devices and operating systems is a major new threat.	Converting users to mobile wallet use and payments appears to foster more security (and user convenience) vis-à-vis EMV deployment, but large-scale safety of contactless modes on devices protected by third parties (i.e., hundreds of telecoms globally) is unproven.	More than two dozen major companies (phone makers, networks, banks, merchants, and third parties) have independent ideas about security modes, and—so far—little interest in seeking standards.
Contactless	Proliferation of contactless modes that require users to 'tap (MSD), wave (NFC/HCE), hover (MST), scan (QR codes), and pose (Beacon/BLE) across a multitude of devices and tokenization options is better than mag-stripe (and perhaps EMV contact cards) but offers no discrete path for industry investment in sustainable and consistent security.	Consumers, who need to be induced to protect themselves with better security habits and behaviors, are being immersed into inconsistent and confusing situations that can lessen the effects of protections, and push security deployers to lowest common denominator path.	Same issues as Wallet providers (above), but push by networks to move from EMV cards to contactless (cards or mobile) expands uncertainty and skepticism of further investments in 'security' by merchants, processors and third parties.

Rationale for Fed as one Central Authority to Provide Platform for Integrating and Supporting Digital Payments

Ideally, operation of an integrating platform for digital payments would be performed by a Central Authority in a way similar to the role it plays today in wires, ACH, and other payment services. The Federal Reserve as a CA operator would reside in it purview over payments and security in accordance with the Monetary Control Act of 1980 and the report of the Committee on the Federal Reserve in the Payments Mechanism published in 1998[9]. Critically important is the Fed's relationships and potential interconnections abroad to facilitate and support robust, efficient and secure transactions across the globe, as well as its unique position as a trusted and objective arbiter of regulated financial services.

The Fed could conceptually undertake development of the Security Integration Platform Systems as a natural evolution of its historical semi-closed network operations for wire transfers and ACH payments, and its adoption of innovative services such SaaS capabilities for smaller FIs to make those payment without dedicated (and expensive) interconnections. As with these services, the Fed's product participation would not be as a competitor to private-sector providers, but as a default provider to fill a market gap where smaller FIs needed or wanted an alternative[10].

Much of the foundational work needed would expand upon activities the Fed is already participating in—namely working with standards bodies and industry participants to determine security needs and solutions. SPTF projects suggested by SAT provide a good starting point. All solutions identified would

[9] Please see Appendix L—Rationale for Fed Involvement in Payments. *(Not provided here)*
[10] SaaS connections for smaller FIs for ACH and Wire Transfer (FedWire) payments (and other financial services) are provided by LendingTools and Bankers Banks; the Fed provides its services at cost plus a return-on-capital equivalent margin.

subscribe to deployment options from more than one Central Authority (CA)—but the Fed would lead the way in deployment to ensure that at least one CA was developed. (The Fed would share its development work with other qualifying CAs that emerged.)

Concept Design of Representative Business Architecture

A partial model for the business architecture of a digital payments integration platform is provided by Australia's Payments System Board in conjunction with ADI (Australian Deposit-taking Institutions) members and service providers. The Reserve Bank of Australia (RBA) provides the settlement and rules for a Clearing Utility and Overlay Services (which begins with a consumer faster payment "convenience" service (Figure 21).

Figure 21. Australia's Digital Payments Integration Platform

3.5. Description of the preferred business architecture

The proposals above lead to the preferred business architecture illustrated in Figure 1, with the initial convenience service as the first overlay service:

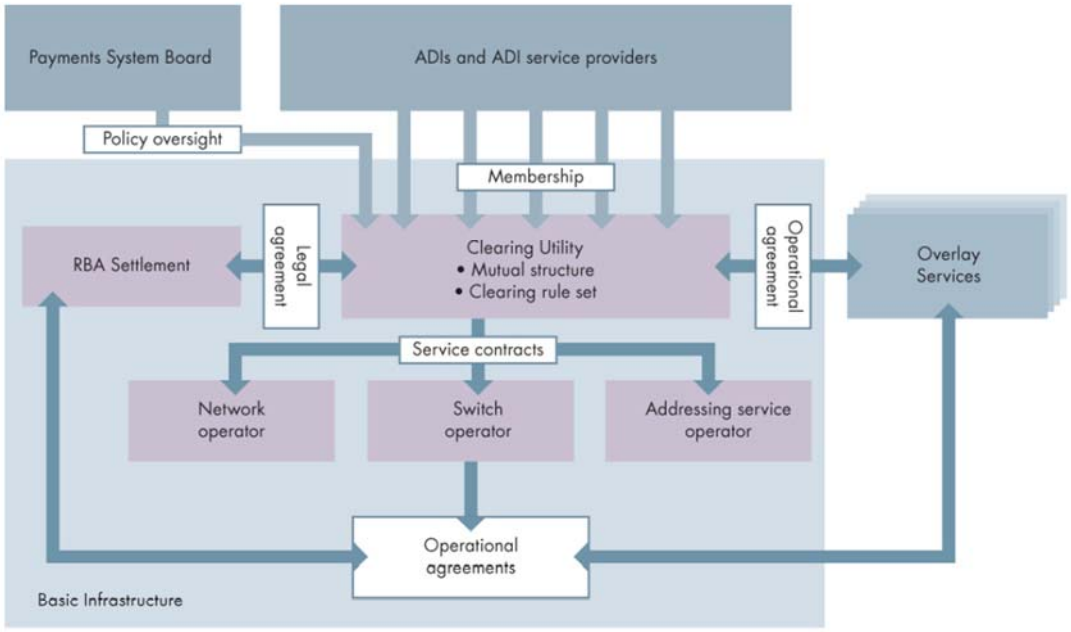


Figure 1. Business Architecture

The basic infrastructure will support all required message flows and associated rules:

- between ADIs and/or ADI service providers;
- between ADIs and the initial convenience service; and
- between ADIs and overlay services.

The detailed business architecture will be reviewed during the initial requirements development and design phase of the RTP Programme. The parties and relationships that make up the preferred business architecture are described below.

The NPP encapsulates a network and operator (SWIFT) as well as a payments-addressing database/service and support for XML-based ISO 20022.[11] Thus, there is a necessary and critical role—and strong precedent—for the Fed to consider in becoming at least one of the Central Authorities tasked with resolving these challenges and problems. SAT stands ready to assist the SPTF and the Fed in pursuing a more secure and efficient payments system in the U.S.

Conclusion: What Happens if Nothing is Done?

The lack of a holistic, analysis-driven assessment of payment security and efficiency, and the potential for new technologies to reduce the escalating threats and damages of cyber-attacks, leaves the nation groping for substantive progress. Examples of decisions that can and must be made abound:

1. **Upgrade to Advanced Encryption Standard (AES) for ATM/Debit Transactions**
   - The Digital Encryption Standard (DES) in triple-applied form protects the ATM debit transacting environments worldwide, but is under constant attack, and will break eventually; Advanced Encryption Standard (AES), which was approved to replace DES in 2002, remains only lightly adopted—owing to the lack of incentives to do the upgrade—including an objective cost/benefit analysis that includes the prospective damages from ultimate compromise.
2. **Upgrade to IOS 8583 (2003 version)**
   - About 90% of U.S. card transactions still operate on ISO 8583 formats using the original *1987* version (which was updated to carry more data—including risk management elements in 1993 and 2003). ISO 8583 is used by most large networks, acquirers, issuers and merchants, but as long as they do not upgrade to the 2003 version, their inability to carry more risk management data for new applications such as needed for chip card transactions results in a 'lowest common denominator' level of security.
3. **Update old ACH formats**
   - The ACH formats are about four decades old, and have proved difficult for many innovators to apply to digital and mobile applications and more rigorous security approaches—even though the ACH network per se is very efficient (25 mils per transaction). Users have embedded application support around these formats for so long that the perceived costs of updating them to 2017 appears enormously uneconomical to some to even consider.
4. **Provide security of additional sensitive data in concert with protecting payment account credentials**
   - Data analytics on transacting information—including user PII, social network access, and account identifiers—are exploding in popularity for identifying more productive customer relationships; but they introduce an abundant new environment for exposure of confidential data, along with a wide array of new providers not yet vetted for their ability to protect users. So, before the nation even gets to the bar for protecting payment account credentials, the bar for addressing additional sensitive data is already being raised;
   - Quantum computing, until recently though by many to be a new threat vector at least five years out, is already upon the nation, and being directed for potential attacks against even

[11] See Appendix K. *(Not Provided here)*

the most protected data centers (including 'clouds'). Without near-term protection of all sensitive data, nothing appears to be safe in the future.

This combination of the albatross of not securing legacy systems for decades with the alarming specter of dramatically more dangerous attack vectors makes doing nothing (or taking a passive stance) seem somewhat reckless to the overall payment system and the economy.
The inescapable bottom line is that the one convening authority that exists—the Federal Reserve—will be needed to continue to pull together all parts of the new payments ecosystem to build on what the SPTF began, in order to design and achieve the required next steps to move the industry forward. Those steps logically include:

- Conducting a detailed inventory of each security challenge (problem) affecting each legacy payment system, as well as new digital/mobile alternatives (especially for faster payments)
- Performing an objective, fact-based and vetted analysis of cost-benefits for fixing legacy payment systems problems vis-à-vis transitioning to new payments alternatives with effective security already built-in
- Convening a payments 'council' with representatives from the entire payments ecosystem to clinically prioritize the most cost- and security-effective initiatives, with programs and incentives designed to encourage adoption
- Providing an integration platform on a default basis to all users seeking access to new security-based payment alternatives, for use until and unless the private sector does not invest in the services needed
- Defining enabling regulations and—as needed legislation—designed to ensure steady transition to more secure and efficient payments throughout the economy.

B. Historical Precedent of Australia's NPP for FedNow

The following section provides a historical treatment of Australia's development of its Faster Payments network (the New Payment Platform, or NPP). Australia has been a global leader in reforming the card payments system, including inquiries, tests and regulatory controls and mandates—the latter of which the Fed does not have (and are not included in this extract for FedNow). But FedNow can benefit greatly by understanding the process Australia went through in developing and delivering MPP: Among other things, the single, secure network 'pipe' remains managed by banks at origin and destination, while payment and funds movement transactions can 'plug into' the pipe (as "Overlay Services'—authored by banks and/or non-banks, with participation in them optional to all.

This review of NPP's history and architecture was done in 2017, and is presented here in partial form (missing the interchange regulatory history of that country) to inform the design and development objections, as well as the bidding process for creating FedNow.

I. Overview

This report summarizes research into Australia's efforts to field a faster payments network and transactional system—efforts that consumed more than decade. Much of the perspective below was developed during a week of interviewing principals from most of the groups mentioned in the summer of 2017. This research included review of materials made available by the RBA, as well as production of documentation that began with the founding of the New Payments Platform (NPP) in December 2014 and the production of the Australia Payments Plan ('the Plan') in February 2015. NPP is a centerpiece of the Plan, but the Plan continues to evolve and extend the Australian payments industry's collaboration into evolving areas such as digital currencies, data-sharing with FinTech firms, and digital identities.

It is tempting to view what Australia has accomplished in modernizing and rationalizing its payments system as something of a 'parallel universe' compared to the struggles to obtain safe and efficient payments in the U.S. Australia, led by a proactive regulator (the Reserve Bank of Australia, or RBA—the central bank) working for the benefit of the entire nation and economy, identified issues, challenges, and opportunities with payments as they arose, and lobbied the major providers to address gaps and foster innovations that have made the country among the most successful transacting economies in the world. Its journey to efficient and effective payments has been studied and emulated by its peers—especially Canada—and as such provides a useful model available for the U.S. to learn from and pursue.

The journey Australia took over the past two decades provides a 'road-map' of sorts for retail payment efficacy in particular (other modernization and reforms of financial services, including investments and insurance, are not addressed in this white paper—though they were important as well). To chart this path, the RBA endeavored at many junctures to enlist the viewpoints from throughout the payments ecosystem (big banks, smaller banks, payments processors, merchants, consumers, etc.). It also appears (and was confirmed in interviews of several principals in July of 2017) that the RBA used its legal mandate for regulating payments to intervene on market issues only when it felt the industry itself could provide no effective alternative. Instead, it endeavored to eschew direct intervention wherever it could use its 'bully pulpit' to nudge contending parties to collaborate with one another in moving forward.

No such regulatory mandate to regulate payments exists for the Federal Reserve to-date, however, though the Fed is required to "ensure the safety and integrity of the payments system"[12], and the Fed provides audit and examination services for bank holding companies[13] And there are other marked differences between the financial services industries in Australia vis-à-vis the U.S.: for example:

- Four large banks control about 80% of most banking services markets in that country, with just 150 smaller financial institutions serving the rest of the market; in the U.S., the top 5-10 bank control similar shares of specific market segments such as credit cards, wire transfers and ACH, but debit cards, mortgages, and other retail banking markets

[12] Please see Appendix C *(not provided here)*

[13] The Fed supervises bank holding companies and others (OCC, FDIC, OTC, and NCUA) supervise other FIs in the U.S.; FFIEC is closest regulatory body for online/mobile banking examinations

are shared somewhat more equitably among some *12,500* smaller regional banks, community banks and credit unions[14].

- By contrast, the U.S. is a much larger market (in many segments, volumes are as much as 10 times that of Australia's), but concentration rates for the top 10 banks range from 60%-90%.
- Comparative credit card use between the countries is also fairly pronounced: Many more financial institutions in the U.S. issue credit cards, most with high rewards levels, and at substantially higher interchange, while Australia uses a low-cost national debit network (EFTPOS) for about a quarter of its transactions

There are key differences in outcomes of the comparative payment systems as well. The U.S. has the most expensive, and most paper-bound payment system in the world[15]. Merchants pay far higher fees for card acceptance than just about anywhere else in the world[16], and have regularly sought redress in courtrooms on high interchange rates and restrictive acceptance rules (including their ability to prevent fraud in the face of ineffectual card network rules that enable continued use of account credentials in-the-clear). U.S. consumers have experienced both rampant fraud (the U.S. produces nearly half the card fraud in the world on less than one-quarter of the transaction volume—nearly all from signature-based cards)[17] as well as billions in overdraft fees from use of signature-based debit cards (a payment product supported only in a few countries outside the U.S.)[18].

And the lack of any tangible regulatory mandate over payments has produced a steady stream of court cases against the card networks and major bank issuers since 1998; between 2000 and 2010, Visa and MasterCard have experienced judicial fines of more than $24 billion; but that amount is less than half of any single year or interchange imposed on merchants over that decade. As one of the last significant countries to deploy of chip-based cards (EMV), the U.S. implementation has been acrimonious, frustrating and incomplete. So *laissez faire*, let-the-market-do-it alternative to 'enlightened regulation' is certainly not an effective solution to the high levels of fraud, risk and industry dysfunction that continues to persist.

Yet payments are pretty much still payments, and until the past few years, most countries shared the same eight basic modes of payments: Cash, Paper checks, Electronic Transfers (ACH), Prepaid, Other Debit Transfers, Wire Transfers, Credit Cards and Debit Cards. A comparison of the relative shares of payment modes in both transaction volume and dollar volume is provided in Appendix B: Economic Analysis and Impacts *[Not Included Here]*. Emerging payment modes such as P2P and digital currencies are still tiny and evolving, but represent potentially huge challenges and opportunities to payment systems worldwide. Faster payment systems for digital transacting must co-exist with legacy payments for perhaps decades.

---

[14] Bank of International Settlements comparative data from 2015
[15] Please see McKinsey & Co. metrics on payments market size and growth for the U.S., and RBA for Australia
[16] Please see RBA graphic
[17] Nilson Report
[18] Please see CFPB updated report on overdrafts, August 2017

Management of the basic eight payment modes remains a perplexing and in several ways a daunting problem for participants—resulting in both security challenges (e.g., counterfeit, fraud, data breaches and cyber-security attacks) and economic upheaval (e.g., interchange lawsuits, financing of criminal activities, impediments to conducting faster and more efficient global business). Clearly, in the absence of regulatory mandates in the U.S., a nuanced pursuit of an Australia-style collaboration roadmap might be the only path to a more efficacious payments system—short of continued litigation.

This assessment of the Australian 'journey', therefore, is aimed at identifying the issues and conflicting philosophies that arose in that country over the past decade and a half, as the RBA pursued an agenda of modernization of the payments system, as well as control of the industry's economics. From this experience, it is possible to make comparisons to many similar developments occurring in the U.S.—particularly with respect to deriving an effective real-time payment system.[19]

When the time finally came to build a real-time, digital payments network, the RBA was able to involve industry groups and fashion diverse boards to assess problems and derive solutions cooperatively to address the inherent industry divisions that face both countries; similar mechanisms could be tried in the U.S. to begin the process of fostering collaboration in this country. And at the genesis of real-time payments in the U.S., in consideration of the Fed's initiative to develop a governance structure (and agenda) that pursues a different path to inter-operation, finding new ways for the payments ecosystem in the U.S. to work together seems inordinately opportune.

Furthermore, the endemic and cascading problems between U.S. banks and merchants/third parties—mainly over interchange rates and the rules that enable the card payment networks to restrict merchant payment choice and obligate them to deploy technology and programs with questionable benefits from either and economic or security standpoint—offer a second 'window' into what the U.S.—and the Federal Reserve—can learn from the Australian experience.

II. Executive Summary—Implications for Faster Payments

As the centerpiece of the Plan, and at the imminent dawning of its commercial operations in late 2017, NPP offers an insightful pathway for getting to faster payments:

1) The RBA, in a prescient consultation with the payments industry, concluded in the early 2000s that Australia needed to move to faster payments in order to remain competitive as an island-based country dependent on global business and tourism. In addition, the RBA noted

[19] Practically speaking, funds underlying payments transaction do not have to move instantaneously. Instead, most 'faster payments' systems emphasize guaranteed or incontrovertible transactions—in real-time, while the funds themselves move in, say 15 seconds to 15 minutes (termed as 'near real-time')

that the banks were clinging to their "30-40-year-old" payments infrastructure and impeding innovations needed to compete on a world stage.

2) By 2006, in order to avoid an RBA intervention by building its own platform the country's Big Four banks[20] acquiesced, and attempted to build their own NPP-like platform. Called MAMBO (Me and My Bank Online…), it failed, and was quietly and unceremoniously closed down in 2009, and terminated in 2011. The failure was due to several factors, but the inability for the four big banks to work out issues even among themselves—including interchange fees—was a primary factor.

3) After another industry consultation and paper on payments innovations in 2011, the RBA invited responses to its paper, which led to the formation of the Real-Time Payment Committee (RTPC)—including APCA, the processor Cuscal and six other organizations—to develop a proposal on how a real-time network could deliver the needed innovations in payments use-cases. The sole completed proposal (ultimately for NPP) was approved by the Payments System Board of the RBA, and the RTPC set about to design and launch the new real-time network.

4) The RTPC solution called for efficiency and collaboration around building the basic network infrastructure, but competition around business applications; the design proposed a business application layer (called "overlay services") to exist on top of the network itself; once big banks and small-FI processors plug into the network platform (not a trivial expense/effort for a larger bank with aging systems), virtually any business application (or payments use-case) can readily be accessed—as each FI chooses. This makes participation optional and individualized—leveraging the secure network underneath.

5) As a network, NPP has now finalized its test program and is expected to go live in November 2017 before a public launch in early 2018. . The first Overlay Service is called Osko (developed by BPAY which is an online bill payment company, however Osko will deliver fast P2P and P2B transactions), and most other prospective use cases are expected to be consumer vs. business oriented in the early days.

6) The total budget for NPP, including the first two years of operations, was an estimated A$150 million (about $115 million U.S.). RBA itself has a seat on the NPP board and owns an equity share in NPP, but is also subject to a capital call.

7) Interchange disputes continue to be a backdrop to the RBA's effort to modernize and make efficient its payment system. The initial NPP use case (BPAY) (NOT FOR PUBLIC RELEASE) is based on the payee and the payer paying equal amounts: about penny each for the RBA (to fund its real-time settlement support), and about 4 cents from each to pay NPP expenses. That makes a baseline cost of about 10 cents, with BPay fees ("interchange") to be assessed on top of that. Osko interchange fees are not a matter for NPP but for Osko. They were controversial at the time but are agreed to prior to launch. There is no interchange for the basic Osko service, and a small fixed (ie not advalorem) interchange for Osko pay with document and Osko request to pay. NPP fees per transaction are is volume based and expected to be say around

[20] The Big Four Banks are Commonwealth Bank of Australia (CBA), Australia and New Zealand Bank (ANZ), National Australian Bank (NAB) and WestPac Banking Corporation (WestPac), which collectively control about 80% of most banking services in the country

6-7 cents per transaction both sides, plus a 1c both sides to the RBA for settlement (as of the time of this research.

8) The NPP board includes one seat for each of the Big Four majors, but currently an equal number elected from other NPP participants (the 150 smaller FIs and their processors) the RBA, , and a couple of independents including an Independent Chair, and requires a 2/3 vote on matters—forcing the two banking groups to cooperate in order to get anything done.

9) On hundreds of issues ranging from the original budget to—now—final pricing), there have been only 3 votes. RBA has lost out on a few things it wanted, but views the interactions as positive and constructive.

10) RBA's Payment System Board approved the Australian Payments Plan in early 2015 That plan embraces NPP, but also has far-reaching strategic mission and vision items, which resulted in the creation of another national organization for payments governance—the Australian Payments Council.

11) The APC is still a work in progress, and depends on a 20-year-old group, the Australian Payments Network (formerly the Australian Payments Clearing Association, or APCA), to do a lot of the operational and tactical legwork—especially on settlement, directories, etc.

12) In each of the three groups (NPP, APC and APN), the progress made is attributed to several factors, including involvement of senior executives with decision-making authority, agreement to and—at NPP—use of a "social contract" for ensuring collaborative behavior, and persistent participation (but not dictation) by the RBA. The invisible hand of the RBA and its threat of intervention is the constant feature throughout everything; but the social contract was important for NPP particularly.

13) The NPP project is and has been project-managed (as well as facilitated) by KPMG, which also managed faster payments projects in the U.K. Unlike those deployments (which used VocaLink, now a MasterCard-owned ACH-based platform, which is also used by The Clearing House in the U.S.), the NPP network is secured by TLS (Transport Layer Security) with full encryption (based on open standards) from originating FI to receiving FI. There is NO data at rest in the network; the FIs are responsibility for the security at either end.

14) Once the Australian banks complete their integration to the NPP network (at a cost estimated at 10 times the original investment in NPP), market forces are expected to drive a business applications, FI and third-party offerings, pricing and usage—helping the APN manage the transition from legacy payment streams in the overall payment mix. the APC has an objective 'managing the payments mix' which is about trying to manage the relationship (read: migration) from legacy payment streams to newer ones.

III. Relevant Historical Timeline and Milestones

Three sets of milestones—depicting the journey taken to payments modernization—are useful to understanding the complexity of the process and the nuances involved in the transition in Australia. The first timeline is the one that appears on the Australia Payment Network (formerly the APCA), which charts seminal events in Australia's formal payments transition from the 1970s to 2014. The second timeline was prepared for the U.S. Federal Reserve to

consider as it prepared to implement the Durbin Amendment affecting debit cards. The third was composed for this paper to track the developments from 2012 to present day pertaining to the creation of NPP and the latest intervention in the marketplace by the RBA—as indicia for the Federal Reserve to assess.

APN/APCA Historical Timeline.

The RBA was created in 1959 to perform central bank functions in Australia and oversee the banking system. In concert with other payments marketplaces, the RBA supported electronic payment technologies early—with ATMs in the late 1970s, introduction of international credit cards in the early 1980s, and PIN-debit at POS in 1983. Australia was also an early adopter of telephone and Internet banking in the 1990s, and the population was an early support of low-cost debit cards in the early 2000s. Australia even had the foresight to create a payment addressing directory (BPAY) in 1997 to facilitate accurate bill payments by phone and (in 1999) via the Internet.

The Australian Payments Clearing Association (APCA, recently renamed and rebranded the Australian Payments Network—APN) was formed in 1992 to consolidate settlement capabilities in the country. APCA/APN's websites lists the key payments milestones in that country:

Australian Payments Milestones*

1977	ATMS introduced
1980s	International CCs
1983	EFTPOS
1986	Cheques Act commences
1988	Polymer notes into circulation
1990s	Telephone and later Internet banking introduced
1992	APCA established (1&2 cent coins no longer minted)
1996	Wallis Enquiry into Financial System recommends new regulatory structure for payments
1997	BPay launched for phone and eventually Internet banking
1998	Wallis Inquiry reforms commence with Payments System Board under RBA; Real Time Gross Settlement system commences for high-value transactions
2000s	Debit cards become increasingly popular
2003:	RBA's regulation of interchange fee begins
2005:	PayPal begins operation in Australia
2009:	ATM Direct Charging regime commences; EFTPOS Payments Australia Ltd established as company to administer the EFTPOS system
2010s	Chip, contactless, mobile banking and online currencies emerge
2012	APCA 20 years old
2013	Payments System Board endorse industry proposal for new real-time payments infrastructure
2014	Australian Payments Council established

* from APCA website

It was the Wallis Inquiry in 1996 that marked the beginning of Australia's journey to payments modernization. That market analysis prompted the RBA move to enable proactive regulation—initiating a process that has included three formal reviews of the payments industry aimed at determining whether and what kind of regulations are needed. The results of this inquiry led to the Payments System Act of 1998, which extended a mandate for regulation to the RBA. Over the next two decades, the RBA found it necessary to 'intervene' proactively in regulating payments just three occasions:

- Cuts in and caps on card interchange, and permission for merchants to impose surcharges for uses on payment cards to users in 2003
- Debit card rate caps in 2006-2007
- Caps on rewards card interchange deployed in mid-2017)

Each time, the RBA acted after concluding that the existing payments marketplace could not achieve what was needed on its own. These interventions are discussed in more detail in Appendix A and B. *[Not Provided Here]*

Federal Reserve Reviews RBA Approach to Help with Implementation of Durbin Mandate.

RBA's transition into proactive regulation of payments was researched by the U.S. Federal Reserve in conjunction with the mandate it received to implement the Durbin Amendment of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. A study by Australian research company TransAction Resources provided a more granular timeline based on key regulatory activities through 2010:

Impact of Australian Payments Reform

Milestone	Date
Financial System Inquiry final report (Wallis Report)	March 1997
Payment Systems (Regulation) Act	1998
RBA & ACCC Joint Study	October 2000
Credit card reform Consultation Document	December 2001
Debit reform process commences	July 2002
Credit card reforms finalised & published	August 2002
Merchant surcharging allowed	January 2003
Regulated credit interchange method comes into force	November 2003
New credit card Access Regime comes into force	April 2004
Debit consultation document	February 2005
Revised credit interchange benchmark	November 2006
Regulated debit interchange & HACR	November 2006
Review of Payment Systems Reforms commences	May 2007
Consultation document	April 2008
Findings of review published	September 2008
Revised standard for EFTPOS interchange fees	January 2010

Timeline of Australian Payment System Reforms

Source: Transaction Resources: "Review of the Impact of Australian Payments Reforms" for Federal Reserve System Docket No. R-1404 22 February 2011

Collectively, these milestones—through 2010—occurred in three distinct phases:

1) Initial reviews of payments—especially fast-growing card payments, which began in 1996 and culminated in credit and debit card interchange limits and the ability for merchants to apply surcharges to consumers for use of credit cards in particular by 2003

2) Imposition of debit card interchange limits and revisions in the network brands' foundational 'honor-all-cards' rules in 2006

3) Another review of the payments systems and the RBA's efforts to reform them in 2007-2008, leading to a new inquiry on how to foster more innovations in payments (in 2010-2011).

The TransAction Resources findings—as presented to the Federal Reserve and summarized below—provide an important baseline and set of realizations of how Australia managed to rationalize payments—just as the Fed was dealing with implementation of its Durbin mandate:

2. Key Findings

The key findings of this paper which are directly relevant to the Federal Reserve's rulemaking process are briefly summarized below.

- Issuers on balance receive no revenue from debit card interchange in Australia.
- While fees on scheme debit (essentially signature debit in U.S. terms) are limited to a maximum of a weighted average of 12 cents, the fees paid are actually much lower because merchants have competitive routing options on these transactions.
- EFTPOS transactions (essentially PIN debit in U.S. terms) have interchange that runs from issuers to acquirers (and merchants) and which balances the fees on scheme debit such that issuers on all debit transactions combined pay and receive about the same total interchange.
- Since the reforms of debit interchange, payment by debit has grown faster in Australia than payment by credit.
- Over the past decade, debit card transactions have increased by 290% and spend on debit cards by 380%.
- There has been stronger growth in new debit accounts since the reforms than there was prior to the reforms.
- Although there is no regular data published on cardholder fees for debit cards, it appears they have declined steadily over the past decade.
- The fact that issuers receive no interchange income from debit cards has not led to any attempt to generate additional income from cardholder fees since the debit interchange reforms were implemented.
- Credit card usage has continued to increase strongly since Australia's reforms of credit interchange.
- Card issuer profitability has not been harmed by the reforms. Issuers have reduced costs and increased efficiency.
- Credit cardholder fees were increasing at a faster rate prior to the reforms than they have since the reforms.
- The Reserve Bank of Australia has concluded that merchants' lower costs are flowing through into lower prices due to the competitive environment in which most merchants operate.
- There are a number of debit card payment systems in the world with no interchange fee which have successfully operated for many years, generally with impressive growth and usage.
- The Directorate General Competition of the European Commission found that card issuing would generate positive profits in 20 out of 25 countries studied even without interchange fee income.
- The trend around the world has been to unbundle the governance and branding functions of card schemes (often called networks or card associations in the U.S.) from processing and routing functions so that merchants/acquirers have free choice in how to route and settle card transactions.

Source: TransAction Resources, 2010

A brief summary and analysis of each of these steps in the 'Australian Journey', with detailed excerpts, are provided in Appendix A: Sequential Inquiries and Conclusions.

Developments Since 2010

But much has happened with respect to regulation of payments since 2010. Additional inquiries into both old and new issues have continued as changes in the payments environment

have ensued—including an embryonic movement of many nations to real-time faster payments systems (which began in the U.K., in 2008 with the Vocalink deployment), and a global shift to push high-end, high-fee rewards cards to recover some of the decline in organic growth that began in 2012.

Some of the key milestones from 2010 to present-time are described below:

Year	Activity
2010	EMV
2011	Contactless
2011-12	FSI Inquiry
2013	RBA's Payments System Board (PSB) supports industry new payments platform
2014	Australian Payments Council formed
2015	National Payments Strategy completed/announced in public documents
2015-2016	RBA inquiry into additional reforms needed
2017	Implementation of rewards card fee caps
2017	Australia's New Payments Platform (NPP) goes live

It is instructive to note that in the years leading up to that date (2006-2009), an unsuccessful effort by the major Australian banks to come up with a faster payments network/system of their own provided renewed impetus to the RBA to push for another model for innovation. A litany of developments leading to Australia's debut of its New Payments Platform (NPP), which occur under a seemingly well-orchestrated set of industry interactions, could prove to be the best example of collaboration that leads to enlightened 'regulation' for the Federal Reserve to consider yet. It is described in the section that follows.

Summary of Key Results and Accomplishments

Historically, the role of a regulator in financial services—especially payments—has been somewhat controversial. Interventions by regulators run a wide gamut of activism—from the European Community's aggressive effort to reduce payment costs (caps in cross-border 30 bps for credit and 20 bps for debit transactions) and increase competition and innovation (i.e., Payment Service Directive-2, or PSD2) to virtual *laissez faire* environment in the U.S. Australia, on the other hand, began a journey to rationalize its payments marketplace in the late-1990s, and by many accounts today (2017), is viewed as one of the world's most progressive and efficient payment 'systems'.

As testimony to that tribute, late in 2017 , a group of the Australian payments ecosystem will conduct a technical launch of the New Payments Platform (NPP)—a state-of-the-art real-time payments network aimed at supporting the new world of digital payments, to be launched commercially to the public in early- to mid-2018. Further, in mid-July, the Reserve Bank of Australia implemented another review and updated policies on payments regulation, including:

- capping individual rewards card interchange at 80 bps—vs. 200 bps or higher rates before
- limiting merchant surcharging to actual costs only,

- applying regulation to 'companion' AmEx cards issued by Australian banks
- and applying interchange caps to commercial cards

Along with the U.K. and some Asian countries, Australia is a heavy user of contactless services, enjoys a low level of payments fraud, and fosters industry cooperation via a number of governing bodies. Finally, RBA is an active participant in industry activities and decisions, including holding a stake in the new NPP. Specifically, some of the chief achievements of the Australian 'journey' thus far are indicative of the far greater industry cohesiveness than exists in the U.S.:

1) Industry collaboration appears much higher than in a number of countries (especially the U.S.), enabling constructive conversations and debates on policies, problems, solutions, and accountability; when discussions bog down, the RBA has a track record of timely and generally constructive intervention

2) Constitution of industry governance bodies tends to be balanced among otherwise competing interests (e.g., big banks vs. smaller one, banks vs. users, acquirers vs issuers, incumbents vs challengers, etc.) under charters that appear to defuse contentious issues—yet provide decision-making mechanisms that ensure resolution

3) Interchange rates continue to recede, yet card issuer and acquirer revenue and profits continue to rise—normalizing the economics of card acceptance for merchants without restricting natural industry growth

4) Primary users of the card payments system—merchants—have the recourse to charge other users—consumers—for their choice of high-fee cards, if merchants choose to—allocating the costs of higher-fee rewards cards in particular to the consumers who benefit from them the most

5) Primary beneficiaries of high-fee rewards card use—wealthy consumers—will not only be subjected to surcharging by at least some merchants, but limits on issuer interchange will induce banks to end the 'arms race' in benefits in favor of more rational expenditures on consumer behaviors that can benefit the issuers

6) Differential surcharging focused on the high-fee/high-end rewards card users and reductions in the amounts of benefits indiscriminately bestowed on consumers who don't need the benefits control a regressive redistribution of income that was channeling an estimated 80+% of benefits to less than 10% of cardholders—paid in part by consumers not using cards or using standard cards (without rewards) as they incurred higher retail prices from merchants attempting to cover their rewards interchange costs

7) Overall, the Big Four Australian banks (which control about 80% of most banking service markets in the country) have continued to fare well financially through the various interventions—constituting one of the most profitable (on an ROE basis) group of banks in the world

8) Smaller banks and FIs (only 155 left as of 2015[21]) have shrunk in population, but managed to gain a stake and voice in the future of payments with equal seats on the NPP board

[21] Bank of International Settlements (BIS) data for 2015

9) Australian consumers—with the burden of arbitrarily high surcharges largely disappearing due to policy changes in 2016-17—are comfortable with payments, and support the RBA's reductions in interchange as a way to help retailers reduce prices overall[22]

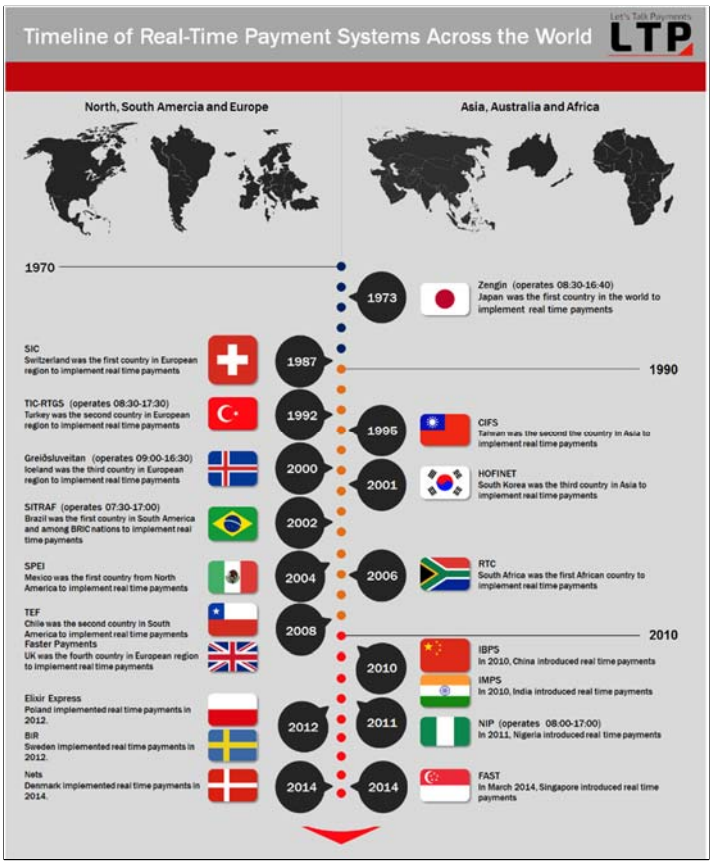
10) Australian merchants—once they have the data feeds to assess specific interchange costs so they can surcharge—are generally comfortable that they are getting a better deal in terms of acceptance costs, and excited about the prospects of getting a highly efficient/real-time payments capability with NPP.

So it should be no surprise that Australia's steady march down the path of rationalization has provided other nations with a vision and expectation for their own efforts at payments reform and rationalization. Canada, for example, conducted its own "Payments System Review" in 2009-2011, modeled in many ways after Australia's (e.g., in 1996-1998, 2007-2008, and later, 2010-2011 focused on innovation). Like Australia, Canada focused on efficient debit payments (avoiding Visa and MasterCard's expensive and fraud-prone signature-debit product), supporting a single EFTPOS national network, aligning banks to play collaboratively, and leveraging digital technology wherever possible. While Canada, which led its reform process through the Finance Ministry, has not committed to a real-time payments system yet, its inquiries and interventions into electronic payment has led them to a comprehensive digital identity initiative—something Australia has also started.

IV. The Real-time Payments Innovation: Genesis of Australia's New Payments Platform (NPP)

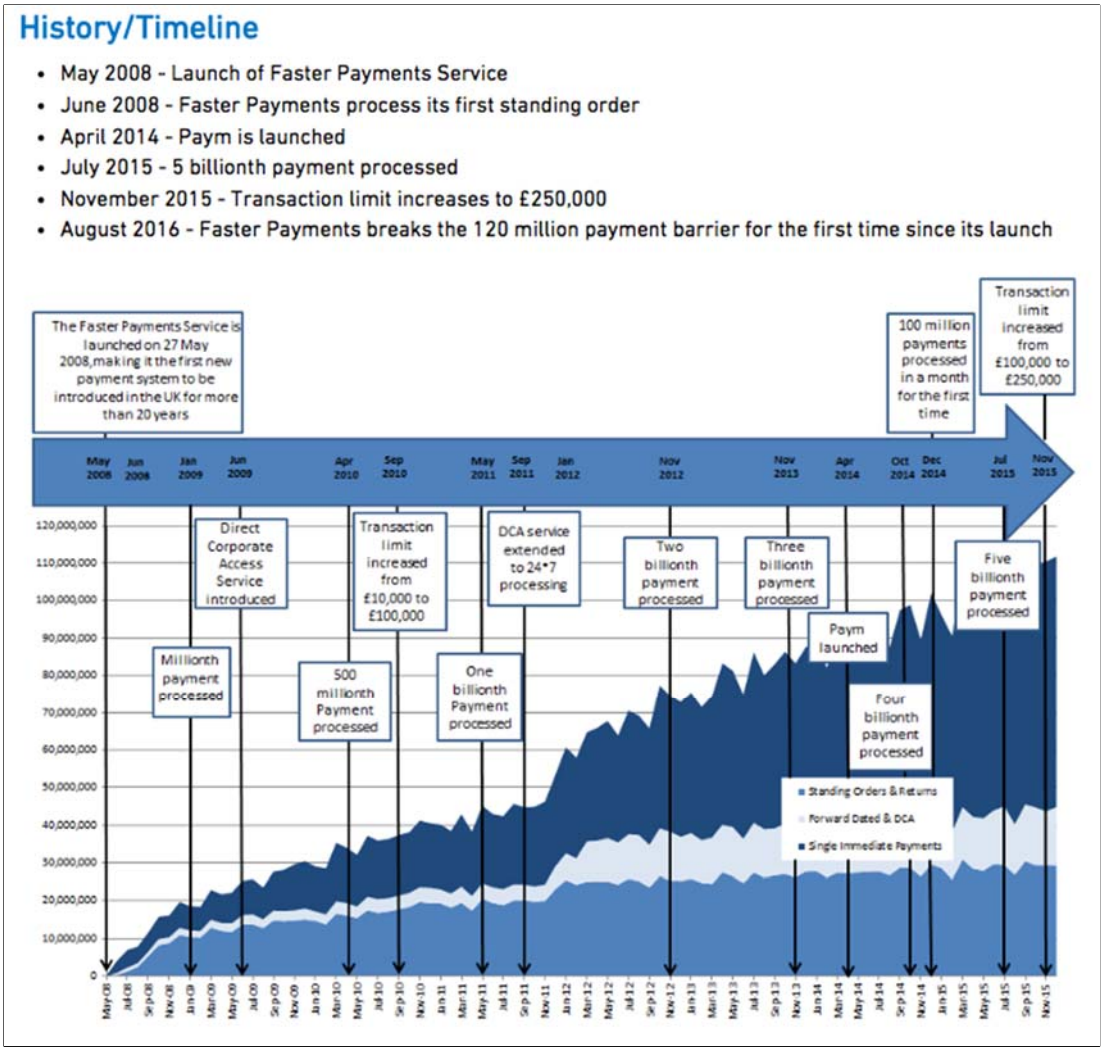
Faster payments, which has received a lot of attention in the U.S. since 2015 when the Fed launched two task forces to consider how to achieve near real-time transactions in this country by 2020, is actually a decades-old phenomenon. The first near real-time payments were conducted in Japan in 1973:

[22] CHOICE, June 2016



But by the mid-2000s, several of the former 'British Commonwealth' countries (e.g, the U.K., Canada, Australia and New Zealand, which were all exploring how to modernize and rationalize their payments systems overall), began to consider real-time payments systems for their countries. Although it was the fourth country in Europe to deploy faster payments, the 'parent' country—the U.K.—raised considerable attention when it launched in 2008 (with the fusion of Voca and Link, a then-dormant secondary ACH network).

It took six years (and 3 billion transactions) for Vocalink to complete the move into commercial operations in the U.K., as it needed to rebuild and re-purpose the old ACH network into a near real-time mode to the point it could launch Paym—the U.K.'s version of mobile P2P payments:



MAMBO—Australia's initial attempt at Faster Payments

Meanwhile Australia, competing for commerce in widespread Asia-Pacific and dependent on tourism, began to consider its own faster payments system in 2006—in acknowledgement of the need to compete more aggressively for corporate/B2B business (as well as to ready the country for digital payments—which were already coming on the scene). RBA published a what was in effect an "innovate or perish" impetus to make a real-time network a reality.

The Big Four banks (Commonwealth, Westpac, National Australia Bank, and ANZ) accepted the 'challenge' and set about a project called MAMBO (Me and My Bank Online) in 2006, in which they were the sole managers. According to a number of observers, governance issues among the big banks surfaced early and persisted throughout the first three years of the project. Among those issues was the inability to decide on what 'interchange' fees to charge.

Originally envisioned as a platform for online payments—namely Australia's BPAY bill payment service with its own biller numbers as a single Internet ID—MAMBO was conceived of as a real-

time P2P and P2B service. But MAMBO's development made little progress, and it was mothballed in 2009. After a 12-month hiatus, BPAY[23] promised to deliver a major portion of the project by 2011, but the Big Four owner banks began dropping out. NAB did so, prioritizing its own innovation agenda, followed shortly by ANZ Bank. BPAY closed down the project for good in late 2011, but successfully transitioned to become the first overlay service ("Osko") on NPP.

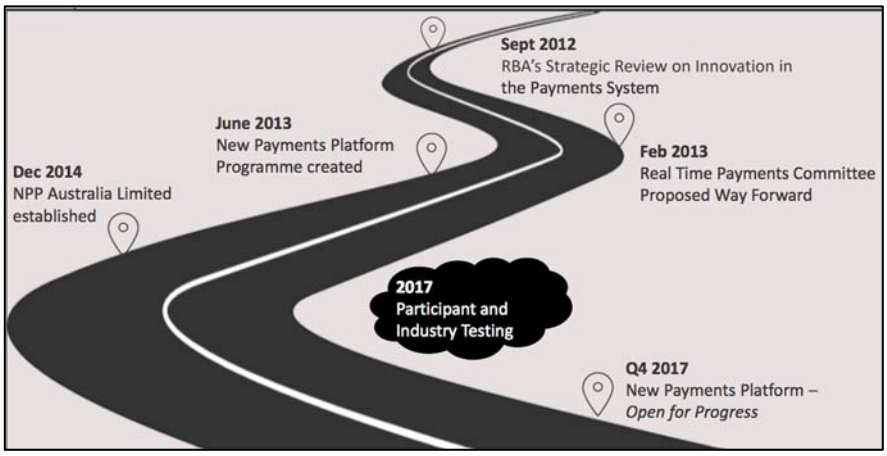
"There were lots of politics," one observer said. "It was too rich of a solution with all the bells and whistles, not just the rails—which were all that's needed to provide the information in the places that were necessary; they were trying to do too much. And they couldn't agree on the interchange fees." In the meantime, according to one source, the failed effort became "a bit of the project whose name can never be spoken" in acknowledgement of the collective embarrassment experienced.

MAMBO's board had been comprised of representatives of just the Big Four banks—"not wide enough involvement", the source said. "It came down to: does innovation work just with the banks, or do you need the central bank on the field? Well, you need the full team on the field!"

NPP (New Payments Platform): Another try at Faster Payments

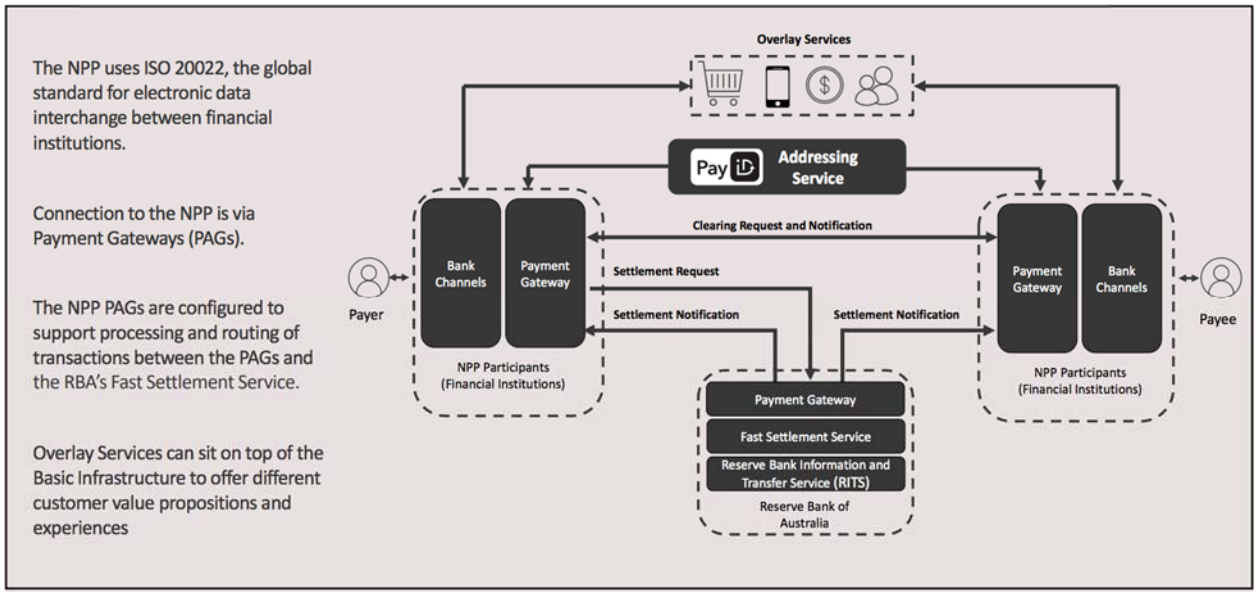
The need for a real-time network had been cited by the RBA in its payments innovation review report in 2011 as a central aspect of the 'next-generation' payments that Australia needed in order to be competitive on the world stage. So RBA continued to lobby behind the scenes for another stab at the project, and by 2013 the successor project—eventually named the New Payments Platform (NPP), re-surfaced to the Payments System Board in the form of the original RTPC proposal was approved, and was launched as a new company in December 2014. NPP was allocated a budget for the development period and two years of operations, and set about building a working system; it expects to go live in late 2017 and be publicly available in early 2018.

[23] BPAY Pty Ltd operates the BPAY Scheme for all its Members and is a wholly owned subsidiary of BPAY Group Limited (previously known as Cardlink Services Ltd.). BPAY Group Limited is owned equally by Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia, National Australia Bank Limited and Westpac Banking Corporation.



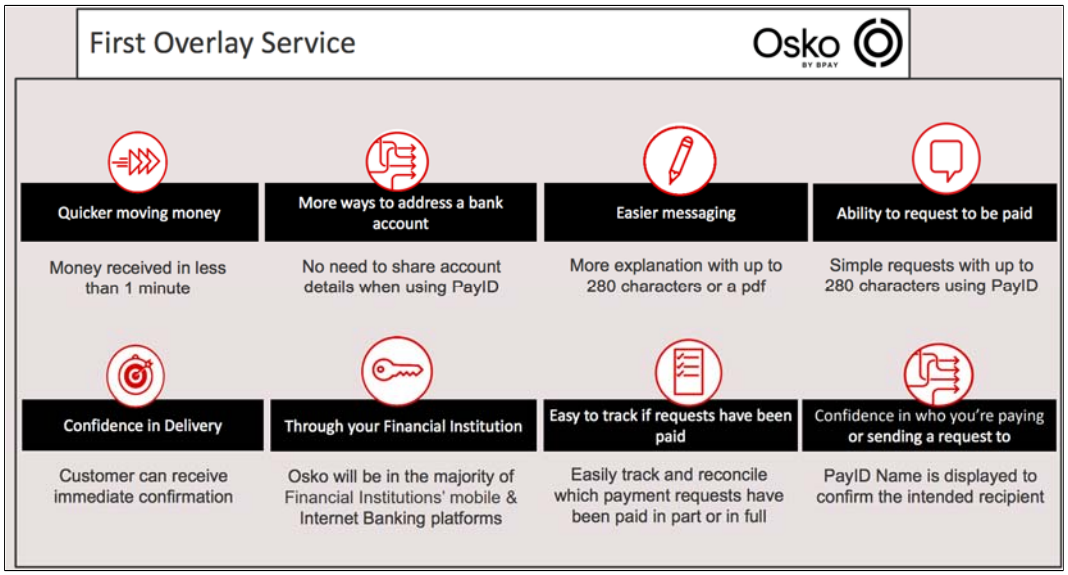
NPP was designed from the outset to foster a level of industry collaboration not present in the initial project (MAMBO). After the RBA's innovation paper, the Australian Payments Clearing Association (APCA) set up a steering committee (the Real-Time Payments Committee, or RTPC) and committed to building the new "rails".

The big innovation in the eyes of many was the design of the system to build "overlay services" (effectively, individual business applications) on top of an end-to-end, secure, digital network component.



This would provide all users and providers with a network utility, but enable banks and third parties to access this network utility in a synonymous way as applications were developed and/or utilized (based on each user's preferences). If a business case can't be mounted for one real-time product, then the rails could support lots of other products that might. That architecture creates a single point of integration, with the attendant ability to pick and choose which applications ("services") to participate in.

The initial overlay service (Osko by BPAY) was designated to facilitate real-time bill payment through the Big Four's BPAY operation:



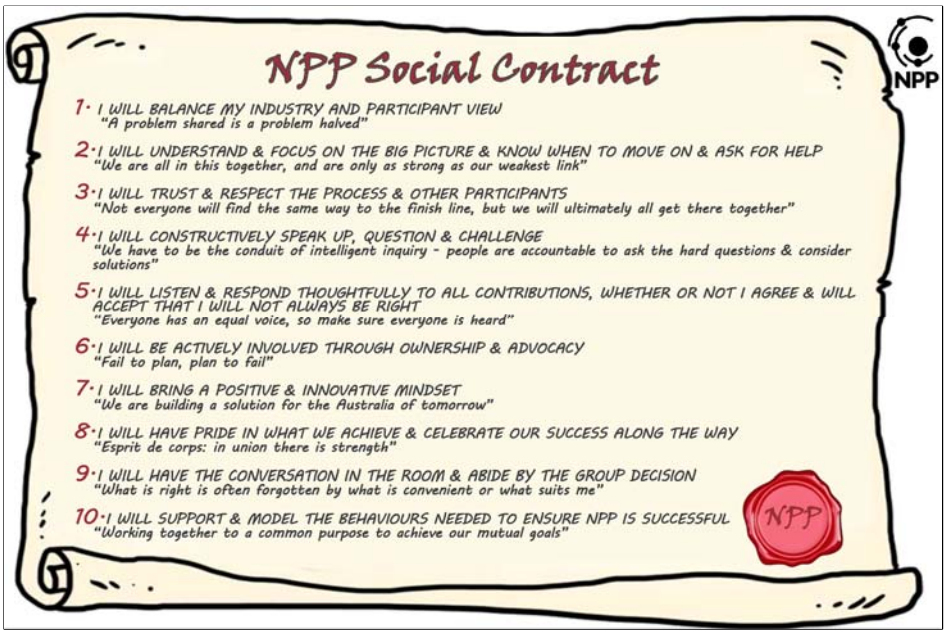
However, getting the big banks to commit to funding and helping to develop the new system was not a trivial undertaking. "There was a building frustration among payments users that the system wasn't innovating fast enough," one observer said. "RBA was intent on achieving a new system without hard regulatory power—purely through persuasion and participation. RBA sought a position on the steering committee and (eventually) the project board." The threat they posed was that RBA would build its own (or PayPal or Google would build it).

"Banks hadn't achieved what they or the RBA wanted to (with MAMBO), but had been given ample opportunity. Some senior (bankers) said there was still no business case for (NPP). RBA countered with 1) you (the banks) are the core payments providers in the country, but you can't continue to say that it's OK to keep operating on 30-40 year-old processing platforms—you can't continue with them forever; and 2) you are confident that no one else can compete, but you (the banks) have vacated the field with PayPal et al, so it's already happened. And other jurisdictions were opening up access (to these new competitors)—as with PSD-2 in Europe.

"The RTPC came back with the proposal for NPP), but there was still some nervousness about what RBA would do. That was understandable, and it worked well to keep things moving. Plus, there was an agreed-upon vision, from the consultation, with RBA's business requirements clear to everyone. RBA accepted (the RTPC) proposal. There were lots of 'to's and 'fro's', and scope creep—but we were always able to get back to the original vision to keep on track. We had the full team on the field, acting as true partners (using Fedline-equivalent talent); there was a lot of skill there. And all parties could speak fearlessly because everyone was involved (in the project); the smaller (FIs) found it comforting."

Governance Structure for NPP: Designed for Collaboration.

RBA became an owner and shareholder for NPP, and set about pushing collaboration to the extent possible. KPMG, an experienced consultant in faster payments and in Australian financial services overall, was engaged as the project manager and facilitator of all the committees and dialogs that ensued. Several observers say one of the success factors was agreeing upon that vision from the outset and engaging competent people to execute that vision. The key task was fostering industry collaboration free from individual, competitive agendas. The NPP development committee settled on the use of a "social contract" to keep participants working for the benefit of all:

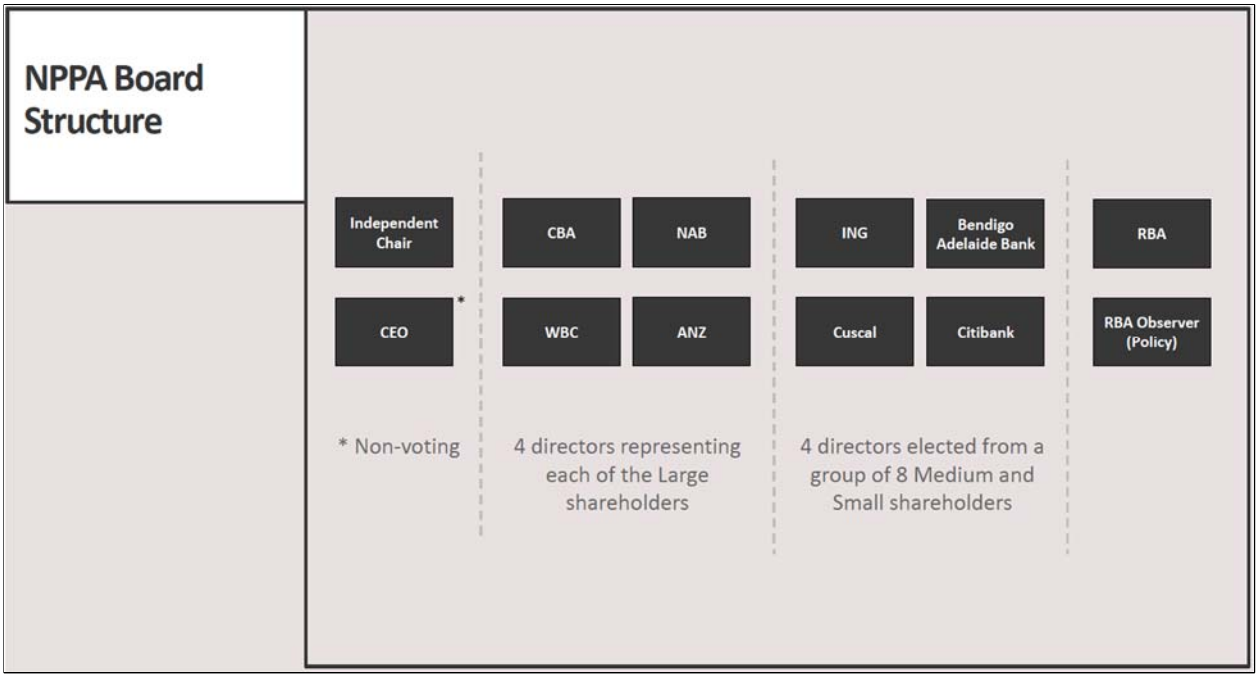


"This was an obligation on the part of participants to bring out the best analysis they could, be selfless and positive in committees, and not to re-litigate issues that had come up before," an observer said. It was also helpful that the banks placed senior people on the NPP Board (executive general manager level, generally). "We wanted them to make decisions on behalf of the company—not just attend all the proceedings as an industry 'representative', which becomes a bit self-fulfilling, rather than decision-making aimed at getting to the next step."."

The NPP Board initially was comprised of one representative from each of the Big Four banks, and an equal number of seats representing the smaller participants. The RBA had a seat (and a shareholder investment), and the 10th and the 11th seats were non-voting—held by the NPP CEO and an independent Chair; (another independent director is being added to make a total of 12). A two-thirds vote is required on debated issues, so the banks must align themselves together to get/defend what they want.

"In the beginning, there were some who were uncomfortable with RBA's involvement, but they've intervened only when it was absolutely necessary," said one observer. "That was

appreciated. And they put operators on the committees, not regulators." The RBA's designated NPP board member is Greg Johnson, Head of Payments Settlements Department, who brings strong operational experience to the table. Tony Richards, Head of RBA's Payments Policy (a portfolio which includes dealing with interchange issues), attends the Board meetings as an observer.



Closely tied to governance, of course, was pricing. For the first Overlay service (Osko), an interchange fee was set by BPay as the first Overlay Service, while network transaction fees are set by NPP. There was no fee intended for Service 1 (the standard speedy payment), and just small fees (less than 10 cents) paid by the sending bank to the receiving bank for Service 2 (pay with document) and Service 3 (request to pay). "They (interchange fees) are only good if you equilibrate them to incent people to join the network," said one source. "They are an absolute nuisance otherwise. If there is a mismatch, it won't work. Some members didn't want to equilibrate on one side artificially winning against the other. Well-trained economists were saying that we needed to move on, while other people were willing just to walk away (from the debate). It was a wobbly moment. But discussion was being had by senior people, not just industry reps (mouthpieces). You need senior people to get an outcome and remain business focused. It helped that the RTPC (Real-Time Planning Committee), the first committee, was senior, and that the RBA Governor was the chair of the Payments System Board, which had accepted the committee's proposal."

The NPP organization—and the governance—has evolved steadily since 2012. Different committees were needed at different stages of the project—design, procurement, building, testing; only a handful of issues have gone to a vote (perhaps a dozen out of a thousand). RBA

itself has been outvoted on three occasions. Thirteen participants representing a wide swath of the banking industry are formal operators for NPP.[24]

RBA's view of the interactions on the NPP board has been positive. "The KPMG social contact was useful—that set down the rules of the game," said one official. "Participants had to leave their (individual) agendas behind. Small and large FIs already had a tradition of working together (via the APCA), but with four directors from the big banks offset by four directors from the smaller FIs, they were compelled to work together.

The selection of NPP's CEO also offers a clue to facilitating cross-industry working relationships. Adrian Lovney, the GM of NPP, was formerly GM at Cuscal (a Jack Henry-like services provider for smaller FIs). He was selected by a committee, and his pedigree was viewed as an important element for getting NPP off the ground successfully—particularly his experience with the smaller FIs.

Budgeting for the long haul was another key success factor. MAMBO had an initial budget of A$227 million, while NPP was initially funded at A$150 million---intended to cover expenses from development through to launch, plus two years of operations. RBA is also funding its development of a real-time settlement system, which is being recouped by a small transaction fee levied on usage.

NPP's Procurement Process: SWIFT Prevails Over VocaLink.

The APCA (under former CEO Chris Hamilton—a key visionary for the project and father of the 'overlay services' innovation) led the effort to put the ultimate design for NPP together. The objectives included data extensions (for better payment instructions), new addressing conventions (for use of mobile phone numbers/emails), innovative standards formats (ISO20022), and 24x7 capabilities.

The initial scoping phase—budgeted at $6 million—invited NETS, IBM, Vocalink (which was said to "have behaved badly during the negotiations, due to perceived arrogance by its American lawyers", an observer noted), Telecom and SWIFT. "Originally, some people thought APCA working with EFTPOS (the national debit network) could do it, but we wanted NPP to have new capabilities, separate maintenance, independent operation—from Day One," one observer said. "Initially, Cuscal and another two companies were involved. PayPal was also there at first, paid $200,000 to look at 1800 pages of requirements, then walked away. ("But RBA still loves them—they offer (meaningful) competition," explained one executive.)

Selection of the supporting vendor for NPP's network came down to Vocalink and SWIFT. VocaLink appeared to have the inside track (due to its deployments in the U.K. and Singapore),

[24] Australian and New Zealand (ANZ) Banking Group Ltd., Australian Settlements, Ltd, Bendigo and Adelaide Bank, Ltd., Citigroup Pty, LTD, Commonwealth Bank of Australia, Cuscal, Ltd., HSBC Bank Australia, Ltd., Indue, Ltd., ING Bank (Australia), Ltd., National Australia Bank, Ltd., Reserve Bank of Australia, and Westpac Banking Corp.

but SWIFT was said to have won out with a more collaborative and partner-oriented approach, along with its considerable experience with network security. "SWIFT is a big company with a lot of recent experience in cybersecurity," said an observer. SWIFT now manages the day-to-day operations, while NPP manages SWIFT and the user community.

"Banks that were doing SWIFT are ahead of the game, but it's a national infrastructure—not a global one," continued this observer. "We did workshops for back-office integration for 8-9 months, and thought about sharing APIs in collaboration, which SWIFT was planning to build for us. In the end, it was between SWIFT and VocaLink, until VocaLink's (American) lawyers got involved. We could have signed with either—500 pages of commercial contract, with variances all explained in them—but once we got to see what their (VocaLink's) lawyers were like, we went another direction."

NPP Funding and Economics.

At the end of the sourcing and budgeting phase, in order to complete the initial funding offer, a drop-dead date for prospective owners was set. One of the Big Four banks missed the date, and it had to be re-set. At that point tensions among participants reached a peak: "There was quite a bit of brinksmanship being played," said one participant. "The (RBA) Governor had to ring up the CEO of one of the biggest banks, and settled the matter with that conversation."

It was also important to get a level of funding sufficient for credibility of the solution. "Cyber (capability and funding) is the distinguishing issue for the individual bank right now," said an observer. "It was essential to contain those costs. TCH (using a VocaLink system) has a fast hub, but it is much more expensive to upgrade the internal switches, the fraud system, account maintenance uplifting 24-7, and the richer data ISO 280-character formats (90% of the cost) like we have now. We won't have that problem."

As with MAMBO, one of the sticking points with NPP has been the cost for users (interchange). "The banks and schemes know where we stand on interchange," said one executive. "NPP knocks it on its head—whether they do it in the overlay service layer—that's up to them—but the fees better not be too high." At this point, the pricing on the basic structure—where the fees are paid equally by the payer and the payee—provides the RBA with half a cent on both sides for settlement services —and that could come down. NPP is expected to charge 6-7 cents per transaction for initial volumes. BPAY sets the pricing through the four majors (e.g., online bill payments at about A$.50 each)—that's a low cost compared to cards, and it's already back-office friendly.

Once that issue is settled, several members of the Australian payments community said they believe there are "huge" business and corporate advantages for credit push payments going forward. "One of the future overlays is a payment request with an attachment 'coming later'; it's just 240 characters of data, so it goes fast," said one executive. "That's the kind of service people want. So we're in serious discussions with senior people to invest in the system."

Additional emphasis is being placed on smaller FIs, and what they can get from the new network. "Smaller FIs participating is a competitive issue in the U.S.," said one participant. "With us, it's a case of accessing particular competing rails: 'Have you agreed what you want to buy?'" If so, the smaller guys can figure out who they want to work with. All the others (faster payments networks) try to set up and let the market decide—that's higher risk. So you make the choice before you start. If you want to buy really good security, and deploy modern message formats, you're talking about (needing to be) a substantial company. And (so) you want the governance super-structure to run it professionally as well.

"You have to understand the fundamentals of the system you want to buy—before you decide what use cases to pursue. Don't just build it for the RBA. We (the NPP) will give you overlays. We couldn't just take the first five use cases from the RBA—we don't even need to know what they are. But they knew enough (being in the middle of the development process) to know they could be accommodated for whatever (use case) comes up. That's future-proofing.". And the reusability of the infrastructure can support multiple use cases—especially in B2B applications, for which users will readily accept reasonable charges (unlike for retail financial services).

The RBA says it had to work hard to get all the majors to agree to fund it. A couple thought internal builds (to integrate to the new network) would be too expensive (they are said to be 10 times the cost of the build for each investor, or A$1.5 billion in total). "A couple of the banks were never true believers." an observer said. "There was no predominant view that real-time is necessary. But we're getting there nonetheless.

"NPP is a win, but there's some fatigue, and some skepticism about the ROI in some quarters. The banks didn't come to the altar willingly—they were pushed by a 'raised eyebrow by the Governor' on what was supposed to be a voluntary choice. That created a degree of discomfort. Banks are accepting (the decision), but it's an enormous project inside each bank. Within each bank there are jaded views, along with accepting parts (of the bank). Banks would be skeptical on the issuing and the acquiring sides. (Operating through) SWIFT will force the banks to invest to update their technology—when the cycles of development are getting shorter and shorter)"

<u>Old and New Governance Structures Adapt: APCA evolves to Australian Payment Network (APN), and the Australian Payments Council (APC) is formed.</u>

The Australian payments system produced an overall Plan for proceeding forward, with leverage from the NPP as a primary driver. The Plan was written largely by the APCA, and published in early 2015.[25] The occasion also produced the introduction of a new governance organization—the Australian Payments Council. "The inquiry of 2011 resulted in three recommendations for same-day payments: 1) enhanced Direct Entry (in 2013), 2) the NPP platform for innovation with data, and 3) momentum for continued innovation," said a source.

[25] Supporting documents for the Plan and the Plan itself are provided in Appendix D *[Not Provided Here]*

Following NPP's debut in 2014, the payments community in Australia decided that a higher-level organization that focused on strategy for payments. APCA, which had been around for two decades, was viewed as more operational, and would help with the heavy lifting for NPP. The new organization, the Australia Payments Council, kicked off in 2015, and has held 3-4 meetings a year since. "The jury is still out on how effective the APC is," said one observer. "but it's looking good so far. The Board of APCA was comprised of industry representatives, not payments experts. That's why they created the APC—for strategic direction and guidance."

The real-time infrastructure they're developing is to enable overlay services. The first one will be BPAY, but another five are expected in the next two years. "In five years, (real-time services) will be viewed as a 'good thing'," says one executive. The banks now want to protect the overlay services, and are trying to decide whether and how to enable FinTech access to customer data. "Third parties can grow volume but the protectionism of existing incumbents—the schemes and the large banks, if not affected by a governance body or regulatory presence, will create a separate economy of internet banks and physical banks like in China," said one official

"These types of decisions shouldn't be made by the will of the small or the large banks. You have to make sure there's a diverse oversight committee. That's why the APC has a broad representation. Many of the seats are rotated (among banks, retailers, PWC, smaller banks). Setting up the APC was a good idea. Has the Council done anything that the APCA board wouldn't have done? It has. For example, they organized a hackathon where the participants wanted access to NPP, Microsoft and other resources. We wouldn't have done that before."

The APC is also focusing on things not attended to previously (e.g., digital identity); what to do with cheques (though cheque volume dropped 20% in the past year); and data sharing. At first, the APC was going to be industry-oriented, not end-user (who typically think payments should be free) based. We looked at the U.K.'s Payments Council, and it appeared not be successful. Instead, the end-users would be represented by the RBA Payments System Board. But technology providers can be involved in the APC. The goal is to deal with holistic payments services—not just payment processes. This reduces the big bank voice and their ability to stand in the way of things.

"At the APC, industry associations only work with decision-makers, so it's more likely to lead to execution—that's why it was created: to make a step-up, where it delivers a payments plan, and have the APCA execute it. In the payments piece the APC looks at the legacy system how it can be migrated to NPP and other changes in the payments system."

"Now, the Australian Payments Network runs as a secretariat, building the outcomes of the APC. It is critical to have specialists invest the knowledge to make things work. The two-tier structure has the secretariat with the APN board delivering with the APC guidance. If you keep the boards completely separate, it wouldn't be optimal. APN would need consultants—and

those are very expensive. But we're still justifying the two boards, and the banks complain about paying for both."

Moving on to Digital IDs and Data Sharing with FinTech.

Much remains to be done to get Australia to the promised land of a fully digital payments infrastructure. "NPP doesn't have that same representation as the APC. Voting is more balanced, but it's all banks. To enable innovation, you need to get a balance of representation and voting rights. We would like to have more FinTech and independent directors. People paying for infrastructure to join have to pay the same as the big banks—but that's a lot of money, even for PayPal.

"Everyone agrees on the Plan…the tricky waters are with the large-scale investment. It's crucial that the regulator empowers the organization to give it technology. From that standpoint, both the APN and the APC are toothless tigers; they are required to pound the pavement for new projects—like digital identity. The RBA will eventually step in, and has control over the key player—the banks—which can have questionable types of influences, unless we designate what payment mechanism we want. If you play this (opportunity) forward, without the RBA, if the banks support something and others don't, you'll get multiple systems.

Sharing data with FinTec companies is a new challenge. "The competition group (from 2011) looked at (payments and account) data, and talked about the need to share it—it's valuable," said one official. "But you can only share data if you know who you're sharing it with. The chairman of APC (Mark Birrell) is really good—he knows we need to resolve this, and sees RBA as the boss. He didn't know anything about payments—he was just a politician. But he was very good at helping the banks think through the issue, and decide on what data is useful in the public interest.

"Banks will have to give access to data, but the only way to do it right is with digital identity. We all knew this was coming. The Murray financial system inquiry (recommendation #16?) concluded that if you don't have a digital ID framework, you would be in trouble. And the government is not capable of figuring this out. In the Plan, the APC will develop this framework, but the head of the Digital Transformation Office which is in charge of digital identity resigned in a dispute with the Finance Ministry—while still having a $70 million budget. The APC meets on digital IDs on a regular basis. Last meeting, we discussed how The Netherlands banks built theirs out from online, put standards together, and got the online retailers to accept it. We said we should do this, and fund more work. One member said no, and others agreed; they said we didn't spend enough time to make clear what we were doing. The objector was new, and never got the background. But the others just didn't want to spend the money.

"Banks have specialized workstreams—getting rid of checks is their top priority right now. But that means they have to push elderly people to something else, which is really difficult. The

U.K. (industry collaboration) lost its regulatory powers because they didn't to a consultation to deal with the elderly concern. We still have to figure these kinds of things out."

KPMG Project Management Role: Leverage SWIFT for a New Operating and Security Approach.

Oliver Kirby-Johnson heads the KPMG project management team for the NPP initiative. Kirby-Johnson fulfilled a similar role in the U.K. VocaLink project, (previously, KPMG's Kevin Brown had direct involvement in the design and development of U.K. Faster Payments, and became its inaugural Chairman of the UK Faster Payments Scheme in November 2011). He commuted to Australia for three weeks a month from England for nearly four years. Kirby-Johnson has met with the Fed several times, and a number of the big banks in the U.S.

KPMG noted that all of the banks were experiencing the high costs of internal integration, and that was the biggest discomfort they had and the reason for the delays; but the appeal of the overlay service concept helped. They thought about sharing APIs and other infrastructure, but decided not to do it after all.

KPMG said it had been difficult most of the way in getting NPP built: "Individuals were resisting, but the social contract helps reign them in," one consultant said. "There is always such useless fighting over IT specifics—what approach works best or is most familiar—but it didn't matter with NPP. The key success factor was keeping the focus on business requirement, not technology choices. I've given the documents to Sean and other Fed people, but I've never gotten anything back."

The security design for NPP is straight-through network operation, with all data encrypted at the originating FI, and all data remaining encrypted end-to-end until receipt by the receiving FI (which then decrypts the data). This is a similar design for SWIFT itself, where the encryption is done in the Transport Services Layer (TLS) in an updated version. This design differs from VocaLink as implemented in the U.K. and at TCH (which use a point-to-point encryption protocol called IPS (IPSec). The TLS security design is more like how Singapore is being built, and appears to be a more modern concept that insulates the network from the applications (in the overlay services layer).

The key is that the network is never exposed (or liable) and the FIs bear all the responsibility. The receiving bank handles any exceptions, with no network involvement. The rules are made by the network (NPP). "There is no ability to deal with finality or liabilities if responsibilities are crossed," the consultant said. "NPP is not liable except if the network itself is compromised."

Advice for the Federal Reserve: Be in a position to build it.

"Things appear very successful (we've been processing test transactions for months)," said an NPP executive. "But it's been very difficult to get off the ground. The most important thing for the Fed is to not be afraid to become involved. Get senior people involved, and orchestrate them in a collegial fashion. Be very clear about what you want to build.

"Without the backstop of our legal powers, it was damned difficult to get the RBA involved. The 2003 interchange and surcharging initiatives worked because it had a credible threat (of a designation). Faster payments are not a credible threat from an interchange standpoint per se—but it was a competitive *threat.* IF the banks didn't build it, the RBA would (at a standard of post-payments in 20 minutes), but not at interchange rate pricing."

Several observers said the U.S. should leverage what it did for ACH and wires—and assert that "We will build it (a real-time payments system) for banks and users who need it." It's the only leverage you can get. Our banks knew we had these (legal) powers, and concluded that the only thing worse than building NPP was having the RBA do it."

"There were obvious differences in market structure—the designation of power vs. convene and discuss. We have a regulatory with a stick, and you don't. RBA's only done designations three time; the threat forces industry to collaborate: if we misbehave, we will get beaten (by competitors). But we also can't walk away from the table. Everything is done in the shadow of designation. The Fed is a regulator, but it appears to be playing a residual role—that's completely the wrong way around. What we've got is Rafferty's rules—or chaos. We believe that the Fed should be a regulator.

"The Fed's been down to talk to us and ask for advice. We've been dealt with a much stronger hand. We don't have senators that can be captured by the voices of the banks; they can't just go off to cameras to complain. Canberra said we'll stay out of that. The government gets questioned twice a year on policies; the schemes get heard there. But that's where it stops.

"It might help to get the users formally involved as a constituent—and represented—group," an official said. The RBA formed a consumer/merchant group the year before last to ensure it was getting the feedback it needed directly. "If you can't persuade the end-users, you probably shouldn't be doing what you're doing. You have to get them onboard early."

"The Fed should cultivate the end-users. When people go to D.C. to protest what the Fed's doing, they should hear from the end-users. But we don't understand the faster payments path they're on—including how TCH's system was designed. When we put out a call for proposals, we got one-from the APCA, which was credible—not 22. And we took care of the smaller FIs right from the outset." "In the U.S. you're just rolling the dice," another official added.

As one executive concluded: "The Fed should target access and ubiquity, and their role in providing it. We put the four major banks in a room together for three years—when they saw it as an advantage to build it themselves. Deloitte did the post-mortem (on MAMBO); the key takeout was the (lack of) government involvement. You could see the Stagegate approach with money allocated with no real clarity about opportunities to review and pull back (constructively). One bank pulled out after 12 months—and so a review was needed.

"The Big Four don't trust each other. And then there's the Sydney-Melbourne rivalry. It was a tussle. And then the non-Big Four were out. With MAMBO, there was no project manager—so

which of the four have responsibility to perform the governance role? There were a number of occasions where two vs. the other two stalled things out. The ratcheting back didn't happen—it was not an industry project approach. It won't succeed if it isn't."

V. Interchange and Other Regulatory 'Interventions'

A companion issue involving the RBA with the industry has been the central bank's strong hand on setting interchange rates. In 2003, the RBA implemented conclusions from the prior year—after consultations with the industry and considerable friction (including court challenges) from Visa and MasterCard. Rates had hovered around 2% of dollar value, which the RBA concluded was far too high, unduly increasing the overall cost of payments without commensurate value to users. The new rates were set at a weighted average of 50 bps. across an issuer's portfolio. However, the rates would be surveyed for compliance every third year. As a result—according to a number of observers—the issuers would jack up rates in the interim period, especially for high-end premium rewards cards, then manage them back down as the compliance audit neared.

Five years later, as a result of an inquiry in to the impacts of regulatory interventions (RBA also implement merchant surcharging in 2003 and caps on debit card rates in 2006) in 2007-2008, the central bank offered to back away from these regulations in 2009—*if* the industry in effect 'cured' some of its issues. That did not happen, and the regulations continued.

Fast forward to 2015, following another assessment of the impact on the industry of the regulations, the RBA concluded four significant analyses:

- Merchant surcharges not infrequently exceeded their cost of acceptance, so a new regulation was promulgated to limit the amounts to actual costs (the calculation of which RBA provided)
- Competitive access to the market had improved, but remained disadvantaged vis-à-vis the incumbents)
- Bank issued 'companion cards' from American Express would come under the regulations as Australian issuers received compensation commensurate to interchange from this arrangement
- High-fee, high-end rewards card interchange levels were rising about 200 bps and proliferating under the 3-year audit cycle, and needed to be curtailed. RBA imposed an 80 bps cap on any single rewards program, and moved the audit cycle to a quarterly basis to minimize issuer 'cheating' on the aggregate 50 bps limit between audits
- RBA also reduced debit from 12 cents to 8 cents with some caps—with no interchange fee more than 20 bps, or 15 cents.

The RBA's concern was—as it was back in the late 1990s and in the analysis leading up to the 2003 designations—that these programs incented a small portion of consumers to use their credit cards more than they would naturally, in order to get the rewards—in effect producing a

'regressive' distribution of wealth—or subsidy—from consumers using standard cards or payment modes other than cards.

"While you might expect consumer groups to favor card programs that provide benefits to consumers, we viewed this situation a little differently," said an executive from a consumer advocate group in Australia. "There was so much money flowing into these cards, and to such a small number of consumers, that we concluded the programs were increasing costs to *all* consumers as merchants had to raise their prices to cover these costs. That's not productive, when higher cost-of-living is our biggest issue in this country."

The RBA's analysis concluded the same sorts of things, and viewed its follow-on intervention on rewards cards as "evolutionary". "We were seeing rates going up—not at U.S. levels, but going up. We shifted to continuous (quarterly) compliance. Banks can still pay rewards, while some consumers are benefitting from the lower interchange, as merchants can avoid high interchange cards. The Interchange Reimbursement Fee (IRF) pushes banks to push less efficient cards—making too much money to (consider using) a new system that is more efficient—like NPP. We have this very efficient debit alternative (EFTPOS), but it was losing out to clackers (knucklebusters). We concluded that in this kind of market, competition drives IRF up instead of down.

"When we got our regulatory powers in 1998, our focus was on credit cards, where IRF was increasing at 30% a year: it was a new system, and it was growing quickly. Loyalty points were said to be the big reason the market was growing so quickly. We were told if we got rid of interchange, we would get rid of rewards for consumers.

"When we decided to put caps on aggregate interchange, MasterCard took us to court. Our preference has always been to do things by persuasion. But with MasterCard claiming our actions would create a 'death spiral' for the industry, it clearly wasn't going to happen (that way). So we removed surcharge restrictions so merchants could get their money back. The big four banks were not happy, even though they were our biggest acquirers, too. We also made the schemes change their rules to allow acquirers-only. The issuers drove the business, and we had only a few acquirers. Banks were not happy because their issuing sides weren't happy. But until the RBA focused on it, the banks were benign about it.

"There are just two interchange rates basically, one for the clackers, and .8 cents for electronic. We don't think the banks understood (any rationale for) it—they just gave some of it back on rewards. But the schemes were focused on it, and we brought attention to that. The banks didn't like the fact that we were meddling. Some of the meetings with the schemes got just awful—we got called all sorts of names. The schemes were very aggressive—even rude. Some of the personalities were abusive.

"After we finished the initial regulation, a lot of the banks settled down. Visa and MC settled back—though there was a hiccup when we designated the (EFTPOS) debit system. Some merchants were upset; the interchange flowed to the acquirer, and some merchants clawed it

back. But they were behind us on credit. Since then there have been a number of personnel changes at Visa, MasterCard and the RBA."

RBA also had a seat at the APCA Board in this period. "We got flack from some of the banks that thought RBA was conflicted. The experience there wasn't fabulous."

The reaction to the 2016's restrictions on rewards card caps has been muted. "There was very little media reaction or from the industry," an observer noted. Part of that might be relief from a worse outcome that was in prospect. "Early on, we had flagged the possibility of moving to 30 bps on credit as the EC did, but we didn't. The industry *could* live with that rate. RBA concluded that the industry could exist with or without *any* interchange—just rules were needed that were fair and transparent. Cards *can* operate at any level of interchange (e.g., 30 bps in Europe, 180 bps in the U.S.)

"The banks said high interchange encourages innovation. If they don't get it, innovation would be stifled. We look at our market, compared with another market across the Pacific (the U.S.). It was difficult to define where the innovation was. We did an innovation review in 2010 and published the result in 2011-2012. We had government departments complaining as users that they can't get good services out of our banks. Some had to use RTGS for emergency payments because they couldn't get real-time payments; when we announced the innovation review, the context was that we needed full network access to real-time—that was one of the key objectives for innovation.

"We have made the observation that high earners were getting the preponderance of rewards, and this in not attractive from a distribution standpoint. But we won't curtail them all together. We published this finding in the Financial System Inquiry (FSI), and will survey every three years what cards consumers are using (to keep checking for the balance)."