Quinte Financial Technologies®

# Interoperability Across Payments, Open Banking, and Digital Identity

## A Trusted Infrastructure Agenda for the U.S. Financial System

**Paresh Ashara | Sriram Natarajan**

19 Fulton Street
New York, New York 10038

(646) 813-0694
www.quinteft. com

# INDEX


**Executive Summary** ---------- **3**

**1. Background** ---------- **4-5**

1.1 The structural issue

1.2 Why this matters now

**2. Problem Statement** ---------- **5-7**

2.1 Payment fragmentation

2.2 Open banking without full trust architecture

2.3 Identity remains repetitive and fragile

2.4 U.S. market structure makes interoperability harder

2.5 AI is moving faster than governance

**3. International Lessons** ---------- **7-12**

3.1 India: A full-stack model

3.2 Europe: Openness with discipline

3.3 Southeast Asia: Policy-driven connectivity

**4. Policy Recommendations** ---------- **12-15**

Pillar 1: Standards and infrastructure

Pillar 2: Trust, consent, identity, and AI governance

Pillar 3: Resilience, competition, and inclusion

**5. Implementation Roadmap** ---------- **15-16**

Phase 1: Foundation

Phase 2: Infrastructure

Phase 3: Market expansion

Phase 4: Cross-border alignment

**6. Evaluation Metrics** ---------- **17**

**7. Conclusion** ---------- **18**


© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

# Executive Summary

U.S. financial infrastructure is sophisticated but fragmented. Customers can move money through cards, ACH, FedNow, RTP, Zelle, wallets, and bank apps; connect accounts to third-party applications; and verify identity through devices, documents, bureaus, biometrics, and passwords. These capabilities are powerful in isolation, but they often operate as separate systems rather than as a coordinated trust layer. FedNow supports instant payments, and the CFPB's Section 1033 rule creates a framework for consumer financial-data access.

Both address important elements of the financial system, but neither addresses the broader need for interoperability across payments, data, and identity.

This whitepaper argues that the U.S. should treat payment interoperability, open banking, open finance, and digital identity as one policy agenda. Payments move value, open banking moves consented data, and digital identity establishes who is authorized to act. Artificial intelligence (AI) now affects all three layers. It can improve fraud detection, onboarding, categorization, and routing, but it also increases risks from deepfakes, synthetic identities, automated scams, and autonomous financial agents.

International experience shows that progress is possible when infrastructure is designed intentionally. India demonstrates the value of a digital public infrastructure stack that links identity, payments, and consent-based data sharing. Europe shows how regulation can require open access while preserving strong authentication. Southeast Asia has advanced interoperability through policy-led coordination, and the U.S. experience with EMV and ISO 20022 shows the risk of waiting too long to modernize core standards.

The policy objective is not to create one universal platform. It is to build a trusted interoperability framework in which systems can connect, compete, and scale without weakening privacy, resilience, consumer protection, or market contestability.

The paper follows a practical sequence: it defines the fragmentation problem, identifies relevant international lessons, translates those lessons into U.S. policy pillars, and closes with an implementation roadmap and outcome metrics. Its central message is consistent throughout: interoperability should be built as trusted infrastructure.

It is organized around four questions: where U.S. financial infrastructure is fragmented today, what international models reveal about trusted interoperability, which policy pillars should guide U.S. action, and how implementation should be sequenced and measured.

This paper treats interoperability as a trust-design problem rather than a technology-adoption problem. The sections that follow show why faster payment rails, open-banking access, reusable identity, and AI controls need to be governed together if the U.S. wants innovation without greater fragmentation.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

# 1. Background

## 1.1 The structural issue

U.S. financial infrastructure is sophisticated but layered. The country has advanced banks, payment networks, fintech firms, processors, and identity providers, yet these institutions do not always share common technical standards, consent mechanisms, or liability rules. As a result, customers and businesses often navigate different rails, APIs, and verification methods depending on the provider.

These gaps show up in several practical ways. Payment rails are not fully mutually reachable, which means that speed, confirmation, settlement certainty, and dispute handling can vary widely by channel. Open-banking permissions are also inconsistent, and many consent screens remain difficult for customers to understand in operational terms. Identity checks are often repeated across institutions, creating friction for legitimate users while still leaving gaps that synthetic identities, compromised credentials, and impersonation attacks can exploit. At the same time, AI adoption is accelerating across fraud detection, onboarding, servicing, underwriting, and payment routing, but the governance frameworks around model validation, explainability, agency, and accountability remain uneven.

## 1.2 Why this matters now

The case for action is strongest because five shifts are occurring at the same time:

(i) Instant payments are moving from an innovation agenda to a mainstream expectation. The Federal Reserve's FedNow Service enables participating banks and credit unions to send and receive payments within seconds, around the clock, every day of the year, but its value depends on broad reach, reliable connectivity, common messaging, and consistent exception handling.

(ii) Payment stablecoins are becoming a regulated alternative rail for domestic and cross-border value movement. The GENIUS Act created a federal framework for payment stablecoins, and regulated dollar-backed instruments could raise expectations for near-instant transfers, lower-cost cross-border corridors, and 24/7 settlement outside traditional bank networks.

(iii) Consumer financial-data access is becoming a formal regulatory priority under Section 1033, increasing pressure to replace fragmented data-sharing practices with secure, standardized interfaces.

(iv) ISO 20022 adoption is becoming a competitiveness issue. The U.S. was slow to implement Europay, Mastercard, and Visa (EMV) chip technology compared with many other markets, and the same pattern could repeat if institutions treat ISO 20022 as a format-conversion obligation rather than as the data foundation for faster, richer, and more interoperable payments.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

(v) AI is expanding both the opportunity and the risk environment. It can make financial services more responsive and efficient, but it also enables fraudsters to scale impersonation, document forgery, account takeover, and social-engineering attacks in ways older control models were not designed to manage.

If these changes happen in silos, the system could become even morefragmented. But if they are coordinated well, they can help build a financial system that is more open, competitive, inclusive, and secure.



## 2. Problem Statement

### 2.1 Payment fragmentation

The U.S. offers many payment options, but they do not interoperate smoothly for customers, businesses, or financial institutions. A payment may move instantly within one network but become slower, less transparent, or harder to reconcile when it crosses another rail, provider, or operational boundary. That variation creates uncertainty around fees, posting times, return rights, fraud handling, and payment-status visibility. FedNow is an important step because it provides instant payment infrastructure with around-the-clock settlement for participating institutions. But instant capability within one service is not the same as ecosystem-wide interoperability. The broader policy challenge is to make payment initiation, confirmation, settlement, exception handling, and remittance information consistent enough for users to trust a payment regardless of the provider or rail behind it.

Stablecoins and ISO 20022 add urgency because they address different layers of the same fragmentation problem. Regulated payment stablecoins could create faster 24/7 settlement options and new cross-border corridors, but they also require coordination around redemption, reserve quality, wallet identification, on- and off-ramp providers, sanctions screening, fraud controls, and dispute handling. ISO 20022 addresses the data layer by improving the structure of payment messages through richer fields for parties, purpose codes, remittance information, status updates, and compliance screening. If stablecoin settlement evolves without common data standards, it could become another disconnected rail. If ISO 20022 is implemented only as a message-conversion exercise, it will not solve operational fragmentation. The opportunity is to use ISO 20022 as the common instruction and reconciliation language while allowing bank-account rails, instant-payment systems, and regulated stablecoin arrangements to coexist under consistent rules for transparency, traceability, and consumer protection.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

## 2.2 Open banking without full trust architecture

Section 1033 of the Dodd-Frank Act is intended to improve consumer financial-data portability by requiring covered institutions to make certain data available electronically to consumers and authorized third parties. This is an important foundation because it shifts the market away from opaque data access and toward consumer-directed sharing. However, access rights alone do not create a complete trust architecture. Legacy systems can make API migration uneven, screen scraping continues in parts of the market, and consent is often expressed through legal language rather than clear, practical choices. Aggregators and large technology intermediaries can also become new concentration points if standards do not support portability and contestability. The policy task is therefore to make open banking not only technically possible, but also secure, understandable, auditable, and fair across providers of different sizes.

## 2.3 Identity remains repetitive and fragile

Digital identity remains one of the weakest links in the financial infrastructure chain. Customers often have to prove the same facts repeatedly to different providers, and the process can be especially burdensome for individuals with thin credit files, limited documentation, language barriers, or accessibility needs. At the same time, fraudsters increasingly exploit synthetic identities, deepfakes, stolen credentials, and AI-assisted impersonation. A modern identity framework must therefore balance security, privacy, usability, and inclusion. It should help institutions establish appropriate assurance for different risk levels without requiring customers to surrender more personal data than necessary.

## 2.4 U.S. market structure makes interoperability harder

The U.S. interoperability challenge is not only a standards problem; it is also a market-structure problem. Banks are visible to customers, but much of the operating infrastructure sits with processors, core providers, merchant acquirers, issuer processors, data aggregators, and embedded-finance platforms. Firms such as FIS, Fiserv, and Jack Henry connect thousands of institutions and merchants to payment, account, fraud, reconciliation, and servicing capabilities. In practical terms, these providers must modernize before banks and fintechs can deliver interoperable services at scale.

This structure makes the U.S. distinct. Some infrastructure providers have greater operational reach than many banks, yet they also compete with one another across core banking, merchant acquiring, issuer processing, embedded finance, and digital enablement. Interoperability therefore requires more than bank adoption or regulatory intent. It requires processors to modernize message translation, native ISO 20022 handling, API gateways, directory services, fraud-data exchange, settlement reporting, exception handling, and service-level monitoring.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

If those upgrades remain uneven, the market can end up with faster rails but inconsistent reach, weaker transparency, and inconsistent user experiences.

Fintechs and digital banking players add another layer to the transition. Chime, Plaid, Stripe, and similar firms can benefit from more standardized account access, payment initiation, identity assurance, and instant-transfer capability. They may also face pressure on revenue streams tied to proprietary integrations, closed routing, data-access workarounds, or premium instant-transfer services. A durable U.S. framework should therefore make interoperability attractive without assuming that every participant has the same incentives. The policy challenge is to align banks, processors, fintechs, networks, and consumer-protection rules around a common operating model.

### 2.5 AI is moving faster than governance

AI can improve fraud detection, transaction monitoring, document processing, data categorization, personalization, and customer service. It can also help institutions identify unusual payment behavior and reduce manual friction in onboarding. Yet the control environment is not mature enough for widespread autonomous financial action without stronger safeguards. New risks include voice cloning, fake documents, deceptive payment instructions, model-driven exclusion, and AI agents that act beyond the customer's intent. Governance should therefore distinguish between low-risk assistive uses, high-impact decisioning, and autonomous actions that can move money, change credentials, or deny access to essential financial services.

## 3. International Lessons

The international examples below are not models for direct replication. They identify design principles the U.S. can adapt.

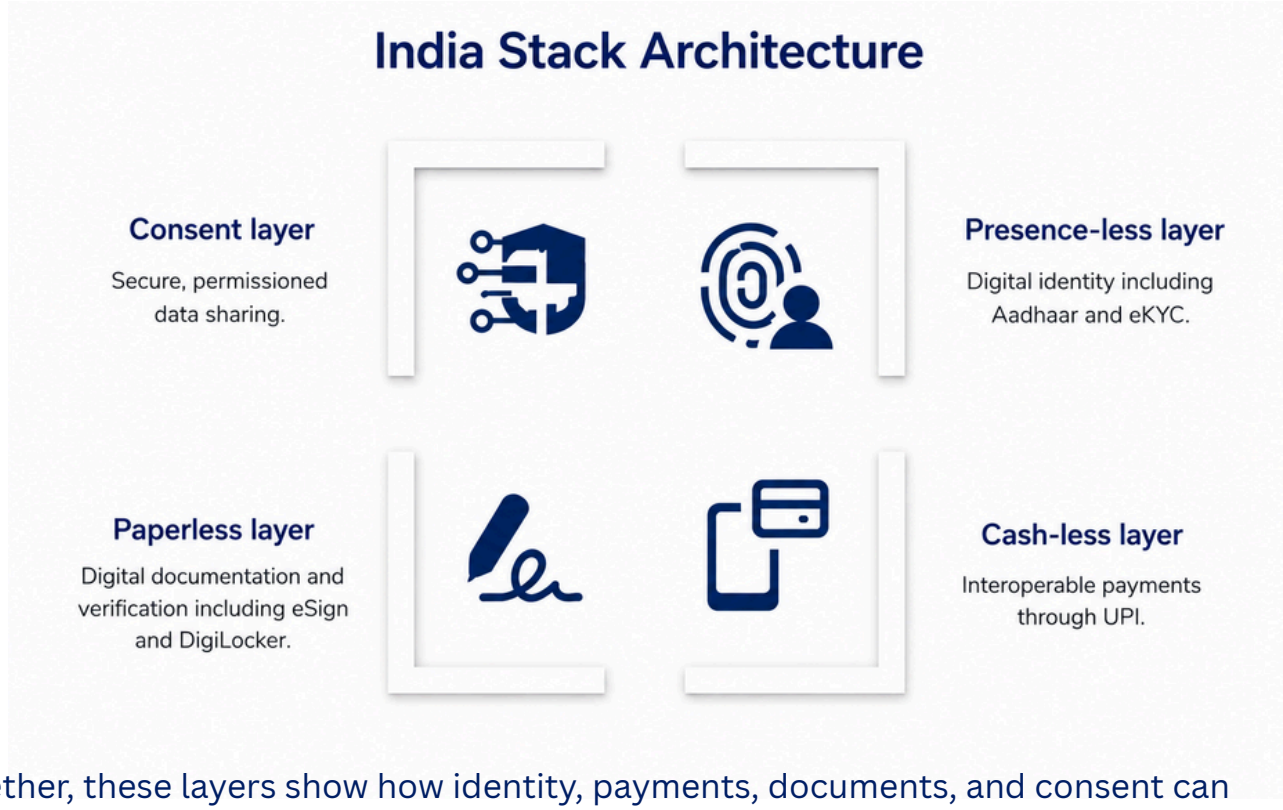
### 3.1 India: A full-stack model

Aadhaar is India's national digital identity program administered by the Unique Identification Authority of India (UIDAI), a statutory authority established under the Aadhaar Act. It assigns residents a unique identity number and enables authentication and electronic Know Your Customer (KYC) processes that can be used, with consent, across government and private-sector services. Over time, Aadhaar has become more than an identification number: it has become a reusable digital identity instrument that supports onboarding, verification, subsidy delivery, account opening, and broader participation in digital financial services.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

India has developed a digital infrastructure made up of interconnected systems known as India Stack, which simplifies complex processes such as identifying account owners and routing payments. India Stack aims to promote financial inclusion and increase competition within financial services. It provides a platform for user-authorized data portability and interoperability across the economy.

India Stack comprises four layers:




Together, these layers show how identity, payments, documents, and consent can reinforce one another instead of operating as separate digital services.
The components of India Stack most relevant to interoperability are Aadhaar, a universal digital identity platform; UPI, an instant retail payment system built on open APIs; common QR standards; and the Account Aggregator framework for consent-based financial-data sharing.

Aadhaar allows identity holders to authorize a bank or other provider to complete electronic verification, creating a digital substitute for parts of the KYC process used during onboarding.

UPI, developed by the National Payments Corporation of India through public-private collaboration, allows individuals to access bank accounts through registered apps and make payments to users of other participating banks and payment providers.

The Account Aggregator framework allows individuals and businesses to securely share financial data with authorized institutions while retaining control over who can access the data, what can be shared, and for how long.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

India's most important lesson is architectural. Its digital public infrastructure connects identity, payments, and data sharing in ways that make financial access more reusable and less document-heavy. The Account Aggregator framework is especially relevant because it enables permissioned financial-data sharing without broad credential sharing.

**Lesson for the U.S.:** Open banking becomes more powerful when it is linked to reusable identity and consent infrastructure.

**Policy implication:** U.S. open-banking rules should be connected to reusable consent and identity capabilities so that data access becomes safer, clearer, and less dependent on repeated credential sharing.

### 3.2 Europe: Openness with discipline

Europe's Payment Services Directive 2 (PSD2 ) regime is one of the clearest examples of regulation being used to open financial-data access and payment initiation while imposing a disciplined security framework. PSD2 required banks and other account-servicing payment service providers to give authorized third-party providers access to payment-account data and payment-initiation capabilities when customers consent. This shifted the market away from bank-controlled data silos and toward a regulated open-banking model in which account information service providers and payment initiation service providers could compete on top of bank infrastructure.

The distinctive feature of the European approach is that openness was paired with Strong Customer Authentication. PSD2's security rules require authentication based on independent factors such as knowledge, possession, and inherence, and they require authentication to be meaningfully connected to the specific transaction or access request. This matters because open banking increases the number of parties involved in the customer journey. Without strong authentication and secure communication standards, broader access could simply create a larger attack surface. Europe's model therefore treats authentication, consent, and third-party access as part of the same trust framework rather than as separate compliance obligations.

The European experience also shows that regulation alone does not guarantee high-quality interoperability. PSD2 created a legal right of access, but implementation varied across member states and across institutions. API quality, availability, consent flows, customer redirection, and dispute handling were not always consistent. In some markets, third-party providers found that access was technically available but commercially or operationally difficult to use at scale. This is an important caution for the U.S.: mandating access is only the first step. A durable framework also needs minimum API performance expectations, testing environments, common data definitions, transparent uptime reporting, and enforcement mechanisms when access is unreliable.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

Europe is now refining this framework through the proposed Payment Services Directive 3 (PSD3) and Payment Services Regulation agenda, as well as broader financial-data access initiatives. The direction of travel is toward stronger harmonization, stronger fraud protections, improved open-banking functionality, clearer liability, and more consistent treatment of non-bank payment service providers. The move from PSD2 toward a more directly applicable and harmonized framework reflects a practical lesson: when markets are deeply interconnected, fragmented national implementation can undermine the very interoperability that regulation is trying to create.

For the U.S., Europe's value lies less in the exact institutional design and more in the discipline of linking market openness to enforceable trust conditions. Consumer-directed data access under Section 1033 should be accompanied by clear authentication expectations, reliable consent records, audit trails, API-functionality requirements, and recourse rules when something fails. Open banking should not depend only on whether a consumer clicked "agree." It should depend on whether the ecosystem can demonstrate that the right party accessed the right data for the right purpose under a revocable and auditable permission.

**Lesson for the U.S.**: Open access works best when it is paired with strong authentication, enforceable API performance, clear liability, and auditable consent.

**Policy implication**: U.S. policymakers should pair access mandates with strong authentication, secure communication standards, API reliability requirements, auditability, and clear liability so that openness increases competition and consumer choice without exposing users to unmanaged fraud, data misuse, or unclear dispute resolution.

### 3.3 Southeast Asia: Policy-driven connectivity

Southeast Asia shows that payment interoperability can advance when public authorities actively coordinate technical standards, market incentives, and regional policy objectives. The region's payment systems have not converged because every market chose the same commercial model. They have converged because central banks and public-sector authorities deliberately connected domestic instant-payment and QR payment schemes in ways that serve trade, tourism, remittances, and small-business payments. This is especially important in a region with diverse banking structures, high mobile-wallet use, large migrant-worker flows, and significant cross-border travel.

A central example is ASEAN's Regional Payment Connectivity agenda, which links national payment systems and promotes cross-border transactions in local currencies. Rather than forcing a single regional payment platform, participating economies have connected domestic systems through agreed standards and bilateral or multilateral arrangements. QR-payments are a particularly visible part of this strategy. Systems such as Thailand's PromptPay, Singapore's PayNow, Malaysia's DuitNow, Indonesia's QRIS, and

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

the Philippines' QR Ph demonstrate how national schemes can preserve domestic control while still creating cross-border acceptance for consumers and merchants.

The practical value of this model is that it reduces reliance on expensive correspondent-banking chains and international card acceptance for smaller payments. A traveler can pay a merchant abroad using a familiar domestic banking or wallet application, while the merchant receives funds through its local acceptance infrastructure. For micro, small, and medium enterprises, this can lower the cost of serving foreign visitors and regional customers. For governments, it supports financial inclusion and strengthens local currency usage by reducing the need for settlement through intermediary currencies for routine regional transactions.

The region is also moving from bilateral links toward more scalable multilateral architecture. The BIS Innovation Hub's Project Nexus is designed to connect domestic instant-payment systems through a standardized model so that each participating system does not need to build a separate custom connection with every other country. Nexus illustrates an important infrastructure lesson: interoperability becomes more scalable when the connection layer is standardized, governance is explicit, and payment systems can reach multiple jurisdictions through a common scheme rather than a growing web of bespoke corridors.

Southeast Asia's experience also highlights the governance work required behind the scenes. Cross-border payment connectivity depends on agreement around participant eligibility, foreign-exchange quotation, settlement timing, transaction limits, fraud monitoring, data sharing, dispute resolution, and consumer disclosures. The customer experience may look simple at the point of payment, but the underlying framework requires careful coordination among central banks, payment operators, banks, wallet providers, compliance teams, and merchants. This is why policy-driven connectivity is different from mere technical integration: it aligns operational rules and public objectives, not just software interfaces.

For the U.S., the lesson is that market choice and interoperability are not opposites. Southeast Asia demonstrates that governments can set the connectivity agenda while allowing banks, fintechs, wallets, and payment providers to compete on user experience, pricing, fraud controls, and value-added services. A comparable U.S. approach would focus on cross-rail reachability, standardized payment-status messaging, interoperable aliases or directories, common QR or request-to-pay conventions, and shared fraud-intelligence pathways. This would not require a single national app or provider. It would require a common operating model that makes the payment ecosystem easier to navigate for customers and businesses.

**Lesson for the U.S.:** Interoperability can preserve market choice while still requiring public coordination around reachability, common messaging, alias resolution, fraud controls, and dispute handling.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

**Policy implication:** The U.S. should not assume that competitive markets will automatically produce interoperability. Public agencies, payment networks, banks, fintechs, standards bodies, and consumer-protection authorities need a coordinated mechanism for cross-rail reachability, common payment-status messaging, reliable alias resolution, transparent foreign-exchange disclosure where relevant, and consistent fraud and dispute-handling practices.

# 4. Policy Recommendations

The recommendations are grouped into three policy pillars to show how individual actions reinforce the same operating model. The first pillar builds shared infrastructure, the second protects trust and customer agency, and the third strengthens resilience, competition, and inclusion as adoption scales.

## Pillar 1: Standards and Infrastructure

### Recommendation 1: Create national interoperability standards

The U.S. should accelerate common standards for payment messaging, API structure, transaction status, identity credentials, and consent records. Interoperability is not only a technical interface; it is a shared language for money movement and data access. Common standards should define core data fields, error codes, status messages, beneficiary verification formats, and assurance levels so that institutions can communicate consistently across rails and services. Payment standards should align with ISO 20022 data practices, particularly for structured remittance information, transparent payment status, exception handling, fraud screening, and cross-border readiness. The U.S. should not repeat the slow EMV migration pattern, where delayed adoption left the market exposed to avoidable fraud and operational catch-up. ISO 20022 should be treated as strategic modernization for faster payments, not merely as a deadline-driven format conversion. Open-banking standards should support secure API access, data minimization, common consent artifacts, and reliable revocation. Identity standards should allow risk-based assurance, reusable verified attributes, and privacy-preserving verification rather than repeated collection of sensitive documents.

### Recommendation 2: Make processors part of the transition architecture

The U.S. payment ecosystem depends heavily on large processors and core providers such as FIS, Fiserv, and Jack Henry. These firms sit between banks, fintechs, merchants, networks, and digital channels, and their operational influence can rival or exceed that of many banks. As a result, interoperability cannot be implemented by banks alone. Processors must upgrade message handling, API gateways, fraud tools, reconciliation services, merchant acceptance systems, and core integrations before many institutions can participate effectively.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

Because these providers also compete across merchant acquiring, issuerprocessing, core banking, and embedded finance, the transition will be harder than a simple regulatory mandate suggests. U.S. interoperability should therefore include processor readiness milestones, common testing utilities, service-level expectations, and migration incentives that make the infrastructure layer a partner in modernization rather than a bottleneck.

## Pillar 2: Trust, Consent, identity, and AI Governance

### Recommendation 3: Make consent specific and auditable

Customers should know exactly what data is being shared, with whom, for what purpose, and for how long. Consent should be specific, revocable, time-bound, and expressed through plain-language interfaces rather than generic authorization screens. A practical consent regime should include a dashboard that shows active permissions, historical access, data categories shared, expiry dates, and the identity of each authorized third party. Revocation should be simple and effective across the chain, including aggregators and downstream service providers. To preserve customer agency, firms should also limit collection to the minimum data needed for the service and avoid using consent as a broad waiver for unrelated monetization or profiling.

### Recommendation 4: Modernize digital identity

The U.S. should move beyond repeated document uploads, weak credential recovery, and knowledge-based verification. Passkeys, hardware-backed authentication, liveness detection, and verifiable credentials can provide stronger and more reusable identity assurance, especially as AI-enabled fraud becomes more advanced. Modernization should not mean creating a single national identity database or forcing every customer into one credential model. Instead, policymakers should encourage interoperable assurance standards, privacy-preserving attribute verification, step-up authentication for high-risk actions, and reliable human recovery pathways for people who cannot complete automated flows. This approach would make identity more secure without making access brittle or exclusionary.

### Recommendation 5: Clarify liability across connected services

Customers should not have to determine whether a failure came from a bank, fintech, aggregator, identity provider, processor, or payment network. The first point of contact should be clear, and reimbursement rules should be predictable. Liability frameworks should distinguish unauthorized access, authorized push-payment fraud, data misuse, credential compromise, technical failure, and payment error. They should also require evidence-sharing among institutions so that investigations do not stall because each party controls only part of the audit trail. Clear timelines for acknowledgment, provisional credit where appropriate, escalation, and dispute resolution would reduce consumer confusion and create stronger incentives for all participants to invest in prevention.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

### Recommendation 6: Govern AI by risk tier

Not all AI use cases carry the same risk. Transaction categorization andcustomer-service summarization are materially different from credit denial, payment blocking, fraud scoring, account closure, or autonomous fund movement. A risk-tiered AI framework should require documentation, validation, monitoring, and human review proportionate to the potential harm. High-impact models should be tested for bias, drift, robustness, explainability, and security vulnerabilities, and adverse decisions should remain contestable by customers. AI agents that act on behalf of customers require additional rules around delegation, transaction limits, auditability, authentication, and revocation so that convenience does not weaken control over financial assets.

### Recommendation 7: Account for fintech and digital-bank incentives

Fintechs and digital banking platforms such as Chime, Plaid, and Stripe stand to gain from interoperability because standardized account access, payment initiation, and identity assurance can reduce onboarding friction and expand addressable use cases. At the same time, interoperability may compress revenues tied to closed data access, proprietary routing, premium instant-transfer fees, and fragmented integration workarounds. Policy should recognize both effects. The goal is not to protect existing revenue pools, but to ensure that firms compete on better products, fraud controls, service quality, and value-added analytics rather than control over closed pathways. Clear standards can help digital players innovate on common infrastructure while preventing new bottlenecks from replacing old ones.

## Pillar 3: Resilience, Competition, and inclusion

### Recommendation 8: Reduce concentration risk

Interoperability should not become a new form of dependency on a few large aggregators, cloud providers, identity vendors, or network operators. Resilience requires multiple pathways, portable credentials, exit options, and tested continuity arrangements. Regulators should monitor critical-provider concentration and require key infrastructure participants to report on operational resilience, cyber controls, subcontractor dependencies, and failover performance. A more connected ecosystem will only be trustworthy if users can continue to transact, authenticate, revoke consent, and access support when a major provider experiences an outage or compromise.

### Recommendation 9: Support smaller institutions and underserved users

Community banks, credit unions, smaller fintechs, and community-based financial providers need practical tools to participate without excessive compliance costs. If interoperability standards are too complex or expensive to implement, the benefits will accrue mainly to large institutions and dominant platforms. Policymakers should therefore support shared testing environments, compliance templates, phased implementation, and technical assistance.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

Inclusion also requires customer-facing design choices: assisted onboarding, multilingual support, accessibility by default, low-bandwidth options, and recovery processes for people who lack smartphones, stable addresses, or conventional identity documents. A trusted infrastructure agenda should expand participation rather than deepen the divide between digitally advantaged and digitally constrained users.

## 5. Implementation Roadmap

Implementation should begin with the trust foundation before expanding customer-facing capabilities. Standards, consent, liability, and AI expectations define the rules under which participants connect. Technical deployment and reusable identity can then follow under a common operating model. Market expansion should begin only after core interoperability controls are tested in real settings, and cross-border alignment should build on domestic maturity. This sequencing reduces the risk of launching faster and more connected services without adequate protections for privacy, fraud prevention, resilience, and customer recourse.



### Phase 1: Foundation

**Primary ownership**: Regulators, standards bodies, payment networks, processors, consumer-protection agencies, stablecoin supervisors, and industry working groups.

**Expected outcome**: A shared rulebook for interoperability before large-scale expansion.

- Finalize interoperability standards.
- Establish consent and revocation requirements.
- Clarify liability and consumer protection.
- Define the role of regulated payment stablecoins in instant and cross-border payment interoperability.
- Set processor readiness expectations for ISO 20022, APIs, settlement reporting, and fraud-data exchange.
- Publish AI governance expectations for financial institutions.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

## Phase 2: Infrastructure

**Primary ownership**: Banks, fintechs, identity providers, API platforms, payment operators, core providers, and merchant and issuer processors.

**Expected outcome**: Secure technical connectivity that applies the foundation rules consistently across providers.

- Expand secure APIs across banks and fintechs.
- Develop reusable identity credentials.
- Implement ISO 20022 natively in high-value, instant, and cross-border payment workflows rather than relying only on translation layers.
- Standardize payment-status messaging.
- Improve fraud-intelligence sharing across rails.

## Phase 3: Market Expansion

**Primary ownership:** Regulated institutions, fintech providers, digital banking platforms, customer -facing platforms, processors, and supervisory agencies.

**Expected outcome:** Broader customer and business use cases built on tested standards, transparent consent, and monitored AI controls.

- Encourage cross-rail and cross-provider portability.
- Expand open finance beyond bank accounts.
- Pilot interoperable account-to-account, instant-transfer, and stablecoin-enabled cross-border payment use cases under clear consumer-protection rules.
- Support customer dashboards and financial-control tools.
- Pilot AI-assisted underwriting and payment routing under strict supervision.

## Phase 4: Cross-Border Alignment

**Primary ownership:** U.S. authorities, trusted foreign regulators, regional payment initiatives, and international standards bodies.

**Expected outcome:** Coordinated cross-border pathways for identity assurance, data portability, payment transparency, and resilience.

- Coordinate with Canada and other trusted partners.
- Harmonize identity assurance and data portability where feasible.
- Improve cross-border payment and FX transparency.
- Build regional interoperability pathways.

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

# 6. Evaluation Metrics

Policy progress should be measured by outcomes, not only by deployment milestones. The test is whether interoperability makes financial services faster, safer, easier to switch, more inclusive, and more resilient in practice. Payment metrics should track speed, cost, reach, settlement certainty, exception handling, reversal clarity, ISO 20022 data quality, stablecoin redemption performance, and cross-border transparency. Open-banking metrics should examine API uptime, data quality, consent comprehension, revocation effectiveness, and customer switching. Identity metrics should assess onboarding success, false rejection, fraud losses, recovery time, and accessibility. Processor-readiness metrics should track native ISO 20022 capability, API performance, reconciliation quality, merchant and issuer integration readiness, and outage recovery. AI metrics should include bias, drift, explainability, false positives, adverse-event rates, and the quality of human review. Competition, inclusion, and resilience should be measured through provider participation, portability, usage by underserved groups, assisted onboarding success, outage frequency, failover performance, and critical-vendor concentration.

| Area | Metrics |
|---|---|
| Payments | Speed, cost, reach, settlement certainty, exception-handling time, reversal clarity, ISO 20022 data quality, stablecoin redemption performance, cross-border transparency |
| Open banking | API uptime, data quality, user consent comprehension, switching rates |
| Identity | Onboarding success, false rejection, fraud loss, recovery time |
| AI | Bias, drift, explainability, false positives, adverse-event rates |
| Inclusion | Usage by underserved groups, assisted onboarding success, accessibility |
| Competition | Number of active providers, portability, market concentration |
| Resilience | Outage frequency, failover success, vendor concentration |

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

# Conclusion

The U.S. has an opportunity to build a financial system that is faster, safer, more competitive, and more inclusive than today's fragmented model. To achieve that goal, it should not treat payments, open banking, digital identity, and AI governance as separate policy conversations. They are parts of the same architecture. Payments move value, open banking moves authorized data, identity establishes who is permitted to act, and AI increasingly mediates decisions and interactions across all three. If these layers evolve independently, the result will be more complexity and weaker accountability. If they are designed together, the result can be a trusted infrastructure layer that supports innovation while preserving consumer protection and system resilience.

The international lesson is not that the U.S. should copy any one model. India illustrates the power of linking identity, payments, and consented data sharing through common infrastructure. Europe demonstrates that openness must be paired with disciplined authentication and liability expectations. Southeast Asia shows that policy coordination can overcome market fragmentation.

The U.S. also has its own cautionary lessons: delayed EMV adoption created avoidable transition costs, and slow or tactical ISO 20022 adoption could repeat that pattern in faster payments. These examples point to a pragmatic policy direction: interoperability works best when it is treated as infrastructure, not as a marketing feature, a private bilateral arrangement, or an optional modernization project.

A trusted interoperability framework would not eliminate competition. It would make competition more useful by allowing customers and businesses to compare services, move data, verify identity, and make payments without becoming trapped in closed systems. It would also help institutions manage risk by creating common expectations for authentication, data access, payment status, exception handling, AI controls, and operational resilience. The policy test should be simple: a more connected financial system must also be more understandable, more accountable, and more recoverable when things go wrong.

The policy direction is clear: interoperability is not inevitable; it has to be implemented deliberately, governed by risk, and continuously adapted as payment technologies, data-sharing models, digital identity, and AI-enabled financial services evolve.




© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.

**Authors:**

**Paresh Ashara** is Vice President at Quinte Financial Technologies, Inc., managing Data Analytics, AI & Automation solutions & services business. He has over 27 years of IT services and product engineering experience in the BFSI vertical. He is passionate about data and advanced analytics and has dabbled in creating solutions leveraging Generative AI and Agentic AI technologies.

**Sriram Natarajan** is President at Quinte Financial Technologies, Inc. He has over 30 years of experience in financial services for credit unions and payment processors. Sriram's extensive experience in the credit and risk industry includes positions with several highly respected organizations, including American Express, HSBC, the National Bank of Kuwait, and GE Money. He holds several professional titles, including Certified Public Accountant, Chartered Global Management Accountant, and Certified Fraud Examiner.

## References

[1] Federal Reserve | FedNow Service overview: https://www.federalreserve.gov/paymentsystems/fednow_about.htm

[2] Security Today | AI deepfakes and fintech identity models: https://securitytoday.com/articles/2026/05/29/ai-deepfakes-force-fintech-identity-models-toward-cryptographic-proof.aspx

[3] India Stack: https://www.indiastack.org/index.html

[4] Consumer Financial Protection Bureau | Personal Financial Data Rights: https://www.consumerfinance.gov/personal-financial-data-rights/

[5] Bank for International Settlements | PSD2, open finance, and authentication policy analysis: https://www.bis.org/publ/bppdf/bispap168.pdf?ck=1776893050

[6] Asian Development Bank | Financial inclusion in Southeast Asia: https://www.adb.org/sites/default/files/publication/222061/financial-inclusion-se-asia.pdf

[7] Bank for International Settlements | Interoperability and payment-system standards: https://www.bis.org/publ/bisbull49.pdf

[8] Cambridge Centre for Alternative Finance | The Global State of Open Banking and Open Finance: https://www.jbs.cam.ac.uk/wp-content/uploads/2024/11/2024-ccaf-the-global-state-of-open-banking-and-open-finance.pdf

[9] European Commission | PSD3 and Payment Services Regulation proposal: https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en

[10] ASEAN | Regional Payment Connectivity cooperation: https://asean.org/wp-content/uploads/2023/05/08-ASEAN-Leaders-Declaration-on-Regional-Payment-Connectivity-and-LCT_adopted.pdf

[11] ASEAN | Regional Payment Connectivity cooperation: https://asean.org/wp-content/uploads/2023/08/Joint-Statement-of-the-10th-AFMGM-Final.pdf

[12] GovInfo | GENIUS Act: https://www.govinfo.gov/content/pkg/COMPS-18221/pdf/COMPS-18221.pdf

[13] Bank for International Settlements | Project Nexus: https://www.bis.org/about/bisih/topics/fmis/nexus.htm | https://nexusglobalpayments.org/

[14] Monetary Authority of Singapore | Regional Payment Connectivity: https://www.mas.gov.sg/news/media-releases/2022/central-banks-of-indonesia-malaysia-philippines-singapore-and-thailand-seal-cooperation-in-regional-payment-connectivity

[15] Federal Reserve | Payment stablecoins and cross-border payments: https://www.federalreserve.gov/econres/notes/feds-notes/payment-stablecoins-and-cross-border-payments-benefits-and-implications-for-monetary-policy-20260330.html

[16] U.S. Faster Payments Council | ISO 20022 implementation and benefits: https://fasterpaymentscouncil.org/blog/13954/U-S-Faster-Payments-Council-Releases-Dual-Reports-on-ISO-20022-Implementation-and-Benefits

[17] Federal Reserve Bank of Kansas City | Market structure of core banking services providers: https://www.kansascityfed.org/research/payments-system-research-briefings/market-structure-of-core-banking-services-providers/

[18] Stripe | Open banking and open banking APIs: https://stripe.com/resources/more/open-banking-explained

© 2026 Quinte Financial Technologies, Inc. All Rights Reserved.