A strategic framework for managing operating and compliance risk in the payments business

David C. Robertson* and Paul LaRock

Received (in revised form): 25th October, 2007

*Treasury Strategies, 309 West Washington Street, 13th Floor, Chicago, IL 60606, USA. Tel: +1 312 6286950; Fax: +1 312 4430847;
e-mail: Dave_Robertson@TreasuryStrategies.com

David C. Robertson *is a Partner in the Financial Institutions practice of Treasury Strategies, Inc., and helps financial services providers improve competitive position, client satisfaction and financial returns. As the head of the financial institutions practice, he helps financial services providers develop payment strategies and solutions. He has led the development of many of the firm's proprietary methodologies in pricing strategies and new product development and is the co-author of Treasury Strategies' groundbreaking whitepaper, 'The Next Generation of Treasury Services'. In addition to his work with banks, securities firms and other financial services providers, David helps technology and service firms understand their target markets, refine their product offerings, position their capabilities, and price to optimise value. He also works with industry groups, regulatory agencies and industry consortiums to maintain their leadership through strategic initiatives that transform the financial services landscape. Prior to joining Treasury Strategies, David spent 18 years in banking, consulting and the public sector. David holds an MA in English Literature from Northwestern University, and a BS in Finance from Indiana University.*

Paul LaRock *is a Principal with Treasury Strategies, and helps multinational corporations and financial services providers to optimise efficiency, understand and manage risk and refine their strategies. Paul has more than 20 years of experience in corporate treasury management and operations. His experience includes policy-making roles in the management of collections, disbursements and liquidity functions. Paul works with corporations and financial institutions to develop practical strategic solutions to the key issues they face. He works for clients with needs in cash management, merchant card processing and treasury technology to increase operational efficiency and internal controls. Paul is a Certified Cash Manager and earned his BS in Accounting and Finance from Eastern Illinois University and his MBA from Northern Illinois University. Paul is a graduate of the University of Chicago's Basic Programme in Literature.*

Journal of Payments Strategy & Systems
Vol. 2 No. 2, 2008, pp. 138–149,

1750-1806

Abstract

A variety of environmental factors have combined to raise the risk inherent in processing payment transactions. Among other factors, risk is increasing because payment methods and channels are proliferating and becoming more complex, settlement infrastructures are expanding access in order to compete, and the velocity and leverage of financial transactions are increasing. In response, regulators have raised the bar, and Boards of Directors and senior management at both banks and other financial services providers are asking tough questions. This paper reviews some of the key forces driving increased operating and compliance risk

in the payments industry and outlines an approach for effectively managing this risk. The authors recommend that payment risk be viewed in its component parts at a foundational level and also offer a more comprehensive framework for risk management that includes not only compliance and control, but also customer experience, efficiency and delivery architecture. Finally, an industry-wide approach to identifying and eliminating risk more rapidly and effectively through a consortium that would share information on payment risks is suggested. This consortium could ultimately also provide a basis for more transparent measurement, monitoring and insurance of payment risk.

Keywords: Risk, compliance, BASEL 2, operations, regulation, channels, networks, controls, architecture, governance, fraud, capital

THE TIMES THEY ARE A-CHANGING

We sometimes fail to recognise the magnitude of change that has occurred because we experience change in small events and gradual increments that appear logical once they have occurred. It is useful, however, to go back just one generation and consider the payments environment that a banker in the early 1980s would have experienced.

Payments were relatively simple in the early 1980s. An individual or business could initiate a payment by cheque, currency and, if they were lucky, by credit card. A select group of special customers could initiate payments by telephone or file. The automated clearing house (ACH) was a somewhat obscure payment method reserved for payroll, recurring debits by large billers, and payments conducted by a small group of firms that used ACH for business-to-business transactions. Most relationship managers knew the commercial activities of their customers intimately and could detect anomalies in payment patterns by simply looking at transactions posting to the demand deposit account.

If one were to take the banker from the early 1980s and transplant him or her to 2007, they would quickly become disoriented by the dizzying array of payment options and processes available in the marketplace. What is more, they might be horrified by some of the payment services being offered. 'How,' they might wonder, 'was something like PayPal ever allowed to happen?'

The relationship manager is now often a capital markets dealmaker who is too busy creating the next deal to reflect upon the debits and credits flowing through their customers' accounts. Automated clearing house has gone from being restricted to an exclusive club to residing at the fingertips of anyone who wants to make a payment. Fast food restaurants, vending machines and taxicabs now accept credit cards, which are sometimes even embedded into procurement and accounts payable processes. And customers can now initiate payments through a variety of channels, including clicking a mouse, driving their car or waving their wallet in the general direction of a wireless receptor.

In order to think about risk in payments, it makes sense to consider payments at the component level, as noted in Table 1. The lists of examples outlined are not intended to be exhaustive.

Channels, payment types, settlement networks and accounts can be mixed and matched together to create new payment solutions — and many payment solution providers appear to be doing just that. The example in Table 2 gives a few extreme flavours of how these combinations might work.

If one conservatively assumes that there are ten channels, ten payment types, ten settlement networks and ten account

Table 1: Payment components

Channels	*Payment types*	*Settlement networks*	*Account*
Channels are the media through which a payment is initiated	Payment types are the form of the payment and define the settlement conventions and regulations governing the payment	Settlement networks are the infrastructure used to exchange funds or information in support of settlement; networks have rules and may limit access	The account is the designated entity to and from which funds are moved
• Telephone • Web • Fax • Card/Plastic • Mobile • Wireless transponder • Mail • File to file • Counter (physical presentment) • –Scanning device + file transmission	• Cheque • ACH (BOC, PPD+, WEB, etc.), GIRO, etc. • Fedwire • SWIFT (eg MT101) • Currency • Prepaid units • Direct account transfer • Credit card transaction (debit, credit, other) • Proprietary payment methods • –Virtual monies (eg Second Life Linden dollars)	• Federal Reserve • Peer to Peer (bank to bank) • ATM networks • Card associations • PayPal • Proprietary • SWIFT • CHIPS • Clearing houses	• Bank demand deposit account • Bank savings account • Bank loan account • Brokerage account • Proprietary accounts (eg PayPal)

types, that results in 10^4 or 10,000 unique payment solutions. Clearly, some combinations are probably infeasible, but one would not rule anything out at this point. As in the example above, someday one may end up imaging currency and converting it to an electronic form of payment or printing currency on our computer just as one does for event tickets.

MANAGING RISK AT THE FOUNDATIONAL LEVEL

Managing the risk of each unique payment solution ultimately becomes impossible for several reasons. First, there is almost no end to the combinations that can be created. Each new channel, payment type, settlement network and account type that is introduced into the market with some unique characteristic has an exponential impact on the number of payment solutions possible. For this reason, the risks of payment solutions must be handled at a foundational level. Some sample risk issues are outlined under the first of the three components in Table 3.

With this foundational approach, the components of payments can be isolated and the risks addressed. This approach also has the benefit of maximising risk management and compliance scale by aggregating the risk and compliance management governance, tools and processes at an enterprise level. This approach also ensures consistency across the organisation, as various units will not treat the risks of specific channels, payment types and settlement networks in an inconsistent manner. Within institu-

Table 2: Sample payment solutions

Channel +	*Payment type +*	*Settlement network +*	*Account type*
Telephone initiated	Reload of a prepaid card	Using PayPal to debit	My parent's bank account
= *Payment Solution*			
Starbucks refill option for slackers who have access to their parent's bank account via PayPal			
Channel +	*Payment type +*	*Settlement network +*	*Account type*
Scanning and file transmission of	Chinese Renminbi notes with unique micro-fibre IDs	Transmitted via SWIFT File Act to credit Walmart's	USD collection account at JPMorgan Chase
= *Payment Solution*			
Remote currency deposit capture solution			

Table 3: Sample risk issues by component

Channel	*Payment type*	*Settlement network*
• Authentication of individual initiating transaction • Permission of individual initiating transaction • Proof that the transaction actually occurred	• Legal and regulatory parameters governing transaction • Rules governing finality and conditions under which transactions may be reversed • Settlement timing, which gives rise to the magnitude and duration of credit risk exposures	• Rules for unwinding transactions in the event of failure

tions, there is a strong likelihood that, should this framework be executed, inconsistencies will immediately be uncovered in the way in which foundational aspects of risk are being managed in different regions, business units or platforms. Generally, these inconsistencies are present in the way the risks of channels and settlement networks are managed, as most banks tend to focus more on the payment type to the exclusion of other payment elements. In addition, fragmentation of channels may result in varying capabilities with respect to control, authentication and reconciliation. Finally, a foundational approach provides a basis for measuring and monitoring risks by component — something that is nearly impossible to do if this framework is not first implemented. Such measurements help prioritise where risks are largest and can thus help guide investments in risk-mitigating tools or education. For example, a bank may view the Web as the primary risk channel and direct most of its risk-management dollars to managing this risk when, in fact, a higher volume of high-risk transactions may be occurring by telephone or other channel.

Consider this foundational approach, for example, in evaluating and managing the risk of the telephone as a channel. In the case of telephone-initiated pay-

Table 4: Sample controls for authenticating payments by telephone channel

Key risk issue	*Preventive controls*	*Detective controls*
Authentication	• Passwords • Callbacks to designated numbers • Recording of telephone calls • Limiting access to payments with some pre-authorised parameters, eg repetitive wires • Voice recognition analysis • Challenge questions	• Detection and investigation of unusual patterns • Post-transaction confirmations
Settlement Timing creating credit exposure	• Deliver versus payment (eg defer outbound payments until covering funds are final) • Pre-fund transactions • Collateralise exposures • Formally approve credit exposures • Identify incoming funds	• Monitor balances and transaction behaviour to flag high-risk exposures • Track incoming payments covering credit exposures and flag for expedited follow-up any exposures that remain open beyond a threshold duration

ments, the bank must authenticate the individual who is initiating the transaction, ensure the person is authorised for the action they have undertaken and, in the case of a dispute, prove that the individual did indeed initiate the transaction. There are numerous types of payment instructions banks can accept by telephone. Rather than individually assess the risk of each type of solution that uses the telephone as a payment channel, it is suggested that banks assess the channel risk and designate appropriate control and mitigants comprehensively and consistently, applying controls based on the magnitude of the risk. Note that this magnitude will depend on other payment elements such as payment type, dollar threshold or a combination of multiple elements. For example, a bank would probably require far more significant controls around telephone-initiated wires over US$1m as opposed to telephone-initiated internal book transfers below US$100,000.

Controls and mitigants can be preventive and detective. Table 4 outlines some sample controls and mitigants for each risk of the channel.

These preventive and detective controls can be developed as a scalable utility across the enterprise. A bank might view voice recognition analysis as economically unfeasible for an individual payment platform, but such an investment might at some point become feasible if leveraged across multiple payment platforms and business units. After authenticating an individual through a challenge question, the system could authenticate the individual thereafter simply by recording their voice.

The bank's operating infrastructure should match the risk framework, scaling all competencies that can be centrally managed. Figure 1 outlines such a framework.

Channels are managed across the enterprise and the affiliated tools, governance and processes around authentication are similarly managed on an enterprise basis.

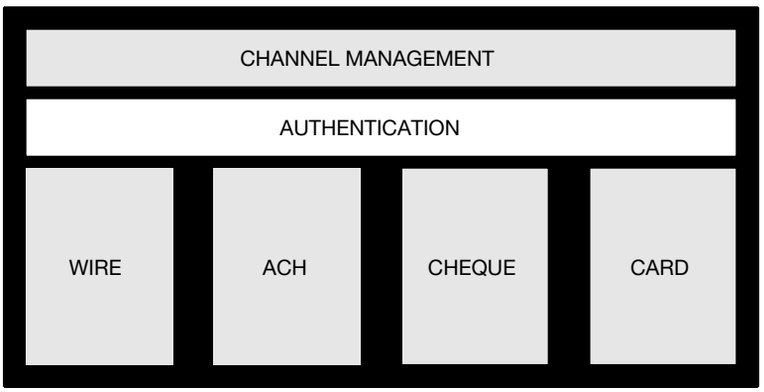

Figure 1 An operating architecture aligned to the foundational risk-management framework

Third party processor risk

This section briefly discusses a critical issue in payments risk — third party processors. Third party processors, such as payroll processors, proprietary settlement networks, collection agencies, etc., pose significant risk because they create multi-channel payment solutions. For example, in the case of a collection agency, they may secure by telephone the approval of a consumer to initiate a debit to a cheque account via ACH and then send that payment instruction to the bank in a bulk file or by initiation over the Web. The bank may authenticate authorised individuals at the collection agency but probably will not authenticate the consumer that originally generated the transaction. Dependent on the nature of the channels, it may be difficult or even impossible for the bank to authenticate the initial payment channel, thus exposing the bank to risk it cannot directly manage.

The risk of multi-channel payment solutions can be addressed through several approaches, which vary in their cost/feasibility and degree of preventive control. At one extreme, banks can demand complete visibility into the activities of their third party processing clients. In the example above, the bank might demand that the collection agency manage its telephone collections with total transparency, using platforms, processes and standards approved by the bank. At another extreme, the bank might simply evaluate the efficacy of the collection agency's internal practices and set limits based on the bank's comfort with the agency's practices and credit condition. In the middle, the bank might investigate the agency's practices, require a SAS70 (Statement on Auditing Standards) Level 1 audit, or have the right to conduct spot audits of underlying documentation on transactions, such as the right to listen to audio files of consumer-initiated transactions or independently verify such transactions.

A BUSINESS VIEW OF MANAGING OPERATIONAL AND COMPLIANCE RISK

Once risks have been appropriately identified and evaluated, a bank must choose among various options as to how best to prevent and/or detect such risks. The same holds true for compliance requirements that must be met. Many business clients tell horror stories as to how risk and compliance management options are selected. One sees business

units faced with the dilemma of either buying technology solutions that are too costly relative to revenues or adding additional staff and costs for manual activities that degrade efficiency and customer experience, while also restricting strategic options by further complicating the delivery architecture. With these challenges in mind, the following framework was developed for assessing operational and compliance risk options, shown in Table 5. Under each element of the framework, an example of a key objective is given and how it might translate to specific metrics or capabilities.

While most risk solutions are assessed based on their ability to limit or reduce operating, credit, compliance and fraud risk, one typically sees very little, if any, attention paid to the impact on efficiency, customer experience and the overall delivery architecture. One finds, however, that these factors are not only worthwhile in their own right, but also heavily interdependent with risk. As a result, by failing to consider these criteria, banks are actually introducing risk back into the system, even as they are trying to reduce it.

Consider, for example, a risk-management solution that impairs efficiency, degrades customer experience and further complicates the technology or processing architecture. While no one would admit to implementing such a solution, one sees these approaches frequently. Inside the bank, they are referred to as 'quick fixes' or 'band-aids'. And indeed, such solutions give the appearance of addressing the risk in question. As an example, a bank whose operation is committing errors may throw more people at the problem to do spot checks to limit errors; however, the fundamental root cause of the operating risk remains unresolved.

HOW RISK SYSTEMS BACKFIRE

Very few banks will admit to being able to tolerate decreases in efficiency — in fact, most are seeking material improvements in staffing throughput levels and unit costs. If a risk solution decreases efficiency, the unit in question will most likely not be permitted to increase its cost structure, but instead will be challenged to cut costs elsewhere to offset the degradation in efficiency. Without any true efficiency gain, the cost cutting will take place by arbitrarily reducing costs — probably staff — increasing stress within the operation and also increasing the likelihood of operating errors or failure to catch errors or fraud owing to staff being overstretched.

In a similar manner, if customer experience is degraded as a result of a risk solution, risks in the system will increase elsewhere. Consider, for example, some of the onerous screening processes a bank may go through to address 'Know Your Customer' requirements. If these procedures are conducted in a manner that starts the relationship off on a bad footing, several secondary impacts are likely. First, sales staff may seek ways to minimise or short-circuit the screening, so as to limit the negative impacts on their client base. Additionally, poor customer experience will cause the most flexible and healthiest clients to seek alternative providers, resulting in an adverse selection in which the bank is stuck with clients who are doing business with the bank because they cannot go anywhere else.

Lastly, the most critical element of this framework is the overall architecture, and this brings us back to the importance of taking a foundational view of risk. Many banks are currently in a vicious cycle where the bulk of their investment dollars are directed toward compliance and maintenance with very little available for net new investment. These investments

Table 5: A framework for managing operational and compliance risk

Risk	*Compliance*	*Customer experience*	*Efficiency*	*Architecture*
Example: Quantification, monitoring and approval of credit risk exposures • Appropriate identification of risks • Quantification of risk exposures relative to nature of risk and customer risk • Monitoring of exposures against limits	Example: Compliance with AML across all relevant platforms • Proper incorporation of geographic, and product risk • Isolation of suspect transactions • Appropriate treatment of high-risk customers and transactions	Example: Service levels relative to customer needs and competitor capabilities • Speed of delivering lockbox images following receipt from Post Office • Elapsed duration to open a new deposit account for an existing customer • Percentage of files transmitted successfully against deadline	Example: Cost efficiency and staff productivity • Unit costs by platform, eg unit costs per wire and per ACH transaction • Throughput rates, eg wholesale lockbox items processed per FTE per month • Key productivity drivers, eg STP rate for wire processing • Cycle times — elapsed process time for an event	Example: Extensibility of platform • Ability to extend risk management and compliance monitoring and filtering across platforms. • Ability to add functionality or third-party integration to existing platforms

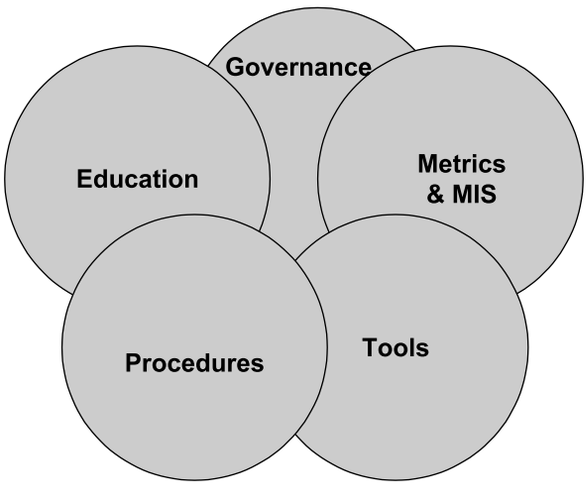

Figure 2 Solution elements for addressing payments operating and compliance risk

are made at the margin — in most cases 'bolted on' to the existing architecture. Each successive round of risk-management investment produces a more complicated architecture such that future development is lengthy, costly and fraught with risk due to complexity. As a result, such institutions are continually strained by compliance and maintenance demands and defer investing in strategic initiatives such as re-architecting their delivery platform.

While such a move might require a two to three year investment window, it could fundamentally free a bank from this vicious circle.

In evaluating options to address risk, it is recommended that banks consider five types of solutions, as summarised in Figure 2.

- *Education* consists of training for staff to ensure they understand risk, are aware of their roles in managing risk, and have the skills and knowledge base to perform those roles. Education should also include an assessment process to validate that staff are positioned to perform their roles.
- *Governance* includes formal oversight of all activities, ensuring that approval decisions are made at appropriate levels of seniority and that decisions are appropriately informed. The scope of decisions should include not only approval of risk exposures and exception activities, but also review and approval of policies and procedures, systems and training programmes. Governance also includes a comprehensive portfolio view as to the optimal risk/return mix of various lines of business.
- *Metrics and MIS* encompasses not only formal *post facto* reports on risk exposures, but also the ability to conduct ad hoc reports or otherwise query a wide array of transaction and customer data for purposes of understanding risk exposures.
- *Policies and procedures* are at the heart of any risk-management programme. Policies and procedures cover not only operating activities, but also risk-management processes, exception approval activities and formal activities to document, investigate and act upon loss occurrences.
- *Tools* are both automated and manual

support materials that assist staff in managing risk. For example, a tool might include something as complex as a cross-platform transaction monitoring system to flag suspicious transactions for anti-money laundering (AML) activities, or it could also be something as simple as a one-page checklist to determine whether a customer is a third-party processor.

Thus, in evaluating options for reducing risks, each of the above five elements should be considered in concert with one another, and the efficacy of the solution should be based not only on the degree to which risk is mitigated, but also on the broader objectives of efficiency, customer experience and architecture.

A VISION FOR THE FUTURE

An unfortunate tenet of risk management is that, as an industry, it tends to learn the hard way. The reasons for this are fairly simple. First, there is no shortage of the creativity of crooks. Secondly, with innovation comes complexity and the potential for unforeseen errors — at times it appears that operating risks follow chaos theory, where the slight shift of a butterfly's wings in South America cause a total crash of a Web platform in the UK.

Banks have made great strides in managing risk across the enterprise. Five years ago, few organisations were able to look at payment risks across platforms. Today, most major banks can do so. Perhaps now the time has come to look at risks across banks. A consortium that provided a clearing house for information around compliance and risk could provide several services.

(i) The clearing house could act as the ultimate AML filter. Properly structured, it could provide privacy to all parties concerned, but filter unusual payment patterns across institutions, thus catching fraud or laundering schemes that were too subtle to be caught at any single institution.
(ii) The clearing house could act as a repository for experienced risks or 'near misses'. The clearing house could operate a clear scheme for classifying risks so that members of the clearing house could do a keyword search on a platform, channel or other term and identify anecdotal information about real-world experiences. The clearing house could produce risk alerts notifying the market of recent schemes or problems.
(iii) The clearing house could provide a structured means for measuring and reporting on risk across the industry. With this information, the clearing house could provide benchmarking data, enabling banks and other financial services providers to compare their performance.

By providing better information and transparency around industry risk, the clearing house would also provide banks and other financial services providers with a quantitative way to present to the market their performance around risk. In turn, this would lead to more informed investment decisions as well as the potential for a secondary market in insuring a broader array of risks. Given the very long tail in some of the risk distributions present in payments, this would greatly strengthen the capital position of institutions.

CHALLENGES TO THE VISION

The financial services highway is littered with failed consortium attempts (does

Table 6: Consortium failures and successes

Failures	*Successes*
• Many players with competing and divergent views or needs • Scope of consortium includes areas seen as potential areas of strategic differentiation • Significant integration costs or challenges in integrating disparate data sets • Exposure of private data to members of the consortium • Potential for collusion or other anti-competitive violations	• Focused group of initial players with critical mass, eg oligopolistic industry structure • Consortium not seen as constraint on competition as area of focus is a commodity • Standards and limited or common points of interface, making integration into the consortium manageable • Limited customer or other critical data or strong protection • No risk of anti-trust concerns

anyone remember EDIBANX?), but there are also successes to which one can point (see Table 6). In general, for a consortium to succeed, it needs to avoid complexity, avoid areas of differentiation and provide a framework for clear benefits.

The above 'lessons' suggest several courses of action for a risk consortium.

(i) The consortium is more likely to succeed if it begins as a small group of large banks coalescing around the concept. Given the consolidation in the industry, three large banks could generate sufficient data to provide a robust sample. For example, in the US, the three largest treasury management banks could generate data on as much as 40 per cent of the payment flows as a party to one or both sides of the transaction, with the total scope dependent on the level of overlap among their transactions. Such a flow would enable them to see larger data samples for pattern analysis as well as produce a transaction risk database.

(ii) The consortium must focus narrowly on risk and avoid tackling issues that would appear to undermine the ability of any player to differentiate competitively. As an example, in the credit markets, the Loan Pricing Corporation (ultimately acquired by Reuters) set out to provide robust data on lending spreads and default experiences but did so in a manner that did not compromise the ability of any individual bank to compete for a particular credit. While risk/return is paramount to business executives, banks will want to differentiate themselves by aligning themselves in varied manners along the risk/return parameter. As a result, the consortium should focus narrowly on risk and not profitability or related revenues.

(iii) The consortium must address differences in data among banks in order to build a robust, universal database. This could be done in several ways. A common technology player in the compliance or risk-management space might join the consortium to provide a proven basis of categorising and mapping data in a manner that supports aggregation across multiple institutions. Alternatively, an industry group could provide a common data framework and possibly also serve as the infrastructure for the activities of the consortium. Examples of

such groups include SWIFT and NACHA.

(iv) The consortium would require a separate legal entity so that the underlying data would be inaccessible to consortium participants. The consortium would also require an infrastructure that provided best-in-class industry standards around data protection. Such a level of protection is critical, as the consortium would necessarily require customer-specific information to be effective. For example, unique account number, bank identifier combinations would be needed to assess patterns across institutions.

In addition to the above challenges, the consortium faces the challenge of resources. Banks are already constrained by investment capital that is all too often absorbed by immediate compliance needs. As a strategic initiative with a payback period of at least 18 months, it is likely that the consortium could be deferred in favour of incremental improvements on a stand-alone basis. One option for overcoming this obstacle would be for a 'for-profit' entity to capitalise the consortium in return for a future profit stream or the initiation of a limited consortium focusing on reporting on experienced risks.

While the above challenges are significant, they are not insurmountable. The authors believe the potential consortium concept should be raised within key industry groups to determine industry appetite and the optimal parameters for such a consortium.

CONCLUSIONS

Payments risk is a quickly evolving arena. New payment vehicles are multiplying, and the card and ACH networks are transforming and competing for additional payment share. Regulators are intensifying their expectations as to the controls and policies that providers have in place. Against this backdrop of change, the authors have outlined an approach for managing payments risk at the foundational level, scaling competencies across the organisation and ensuring greater consistency among business units. A significant risk in managing payments risk is the potential that providers may make marginal investments in risk and compliance controls that negatively affect efficiency, customer experience or the operating architecture of the firm. The authors argue for a broader framework that considers these impacts, which will lead to a more strategic, long-term view of the risk infrastructure, ultimately freeing resources for more discretionary investments. Lastly, a possible industry-wide clearing house to capture and share information on risk and compliance across the industry is outlined. Given the importance of payments risk and compliance, and its potential to 'crowd out' the investments needed to grow and innovate, the authors believe these strategic perspectives and frameworks will best position banks to succeed.