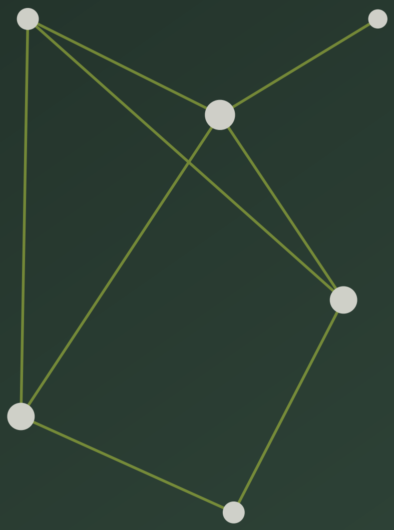
MS ADAPTIVE COMPLIANCE · INSIGHTS



Compliance as a Competitive Advantage

In payments and fintech, compliance is not the cost of growth. It is the infrastructure of growth.

MICHEAL SHEEHY

Executive Essay · July 2026

Payments · Compliance · Leadership

ADAPTIVE COMPLIANCE · EXECUTIVE ESSAY

Compliance Is Not the Cost of Growth

In payments and fintech, the companies that understand risk best are the ones that move faster, earn trust and preserve the strategic freedom to grow.

By Micheal Sheehy

Approximately 12-minute read

For years, compliance in financial services has been described in the language of restraint.

It slows launches. It adds friction. It increases cost. It asks for more documents, more controls and more approvals. It is the function that says no—or, at best, “not yet.”

That view is understandable. It is also increasingly wrong.

In payments and fintech, compliance is not simply a control function sitting beside the business. It is part of the infrastructure on which the business depends. Licences, bank partnerships, payment rails, institutional customers and global market access all rely on confidence that the company understands and can manage risk.

The strongest payments companies are therefore not the ones with the lightest compliance programmes. They are the ones that can identify risk earlier, design around it more intelligently and make well-supported decisions faster than their competitors.

That is the real compliance advantage.

> “The strongest payments companies are not the ones with the lightest compliance programmes. They are the ones that understand risk early enough to move with confidence.

01

THE INFRASTRUCTURE OF TRUST

Payments Runs on Permission

A technology company can build a brilliant product and take it directly to market.

A payments company cannot.

Payments businesses operate through a network of permissions, dependencies and trusted relationships. They need regulators to issue licences. They need banks to hold and move funds. They need card networks, local payment schemes, correspondent partners and settlement providers. They need enterprise customers to complete due diligence and believe the platform can protect their businesses.

This means compliance capability affects far more than the risk of enforcement.

It affects whether a company can enter a market; launch a product; maintain a banking relationship; serve a regulated customer; support a new payment corridor; respond to geopolitical disruption; survive a serious control failure; and earn the trust required to scale.

In payments, trust is not a soft brand value.

It is access to the infrastructure on which the company operates.

A fintech may have faster technology, a better interface or a more innovative product. But if its partners do not trust its controls, growth eventually hits a wall.

That wall may appear during a licensing application, a bank review, an acquisition, an enterprise sales process or a regulatory examination. The company then discovers that compliance was never separate from its commercial strategy. It was embedded in it all along.

02

SPEED THROUGH CERTAINTY

The Real Source of Delay

Compliance is often blamed for slowing the business.

Sometimes that criticism is fair. Some compliance programmes are overly manual, inconsistently governed or unable to distinguish between genuine risk and institutional habit.

But much of the delay attributed to compliance is actually caused by late engagement.

A product team develops a new offering. Commercial assumptions harden. Technology resources are committed. Launch dates are announced. Only then is compliance asked whether the product can proceed.

At that point, every regulatory issue looks like obstruction.

The deeper problem is not slow compliance. It is slow strategy.

Mature organizations involve compliance while the product is still being shaped.

They ask early: What licence supports this activity? Which customers can use it? Which jurisdictions create additional obligations? What data must be collected? What transaction behaviours must be monitored? What restrictions need to exist in the product? Which risks can be mitigated—and which fall outside appetite?

When these questions are addressed early, compliance stops being an approval checkpoint and becomes part of product architecture.

The result is not necessarily an easier answer. It is an earlier and more usable answer.

That creates speed through certainty.

> “ A company that discovers its regulatory constraints immediately before launch does not have a slow compliance function. It has a business-design problem.

03

CORE FRAMEWORK

The Compliance Advantage Flywheel

The competitive value of compliance can be understood as a flywheel. The institution uses risk intelligence to design better controls, improve customer outcomes, build trust, expand access and generate more learning. That learning then strengthens the next cycle of growth.

FIGURE 1

The Compliance Advantage Flywheel

A virtuous cycle that turns compliance intelligence into responsible growth.

Intelligence → Design → Experience → Trust → Access → Learning → Growth.

01

02

03

Risk intelligence

The company understands regulatory expectations, local market realities, customer behaviour and emerging threats.

Compliance by design

Requirements are translated into product logic, customer journeys, data architecture and payment controls.

Better customer outcomes

Legitimate customers face fewer unnecessary requests, fewer false positives and more relevant controls.

04

Trusted execution

Banks, regulators, partners and customers see evidence that the company can manage complexity responsibly.

05

Greater market access

The company can secure relationships, products, licences and corridors that weaker competitors cannot.

06

More data and learning

Growth produces richer intelligence, improving both risk controls and commercial decisions.

07

Faster responsible growth

The organization enters the next opportunity with stronger infrastructure and greater confidence.

04

PRODUCT ARCHITECTURE

Compliance by Design

Every payments company already has compliance embedded in its product.

The only question is whether it has been designed deliberately.

KYC questions, document requests, transaction reviews, account restrictions, payment holds and appeals all form part of the customer experience. They influence conversion, retention and trust just as directly as the interface or the payment speed.

Poorly designed compliance often results from confusing standardization with uniformity.

A global company may create one document checklist and apply it everywhere in the name of consistency. But customers do not live in a uniform world.

A bank statement may be a common proof of address in one country and unavailable or meaningless in another. A small business may operate from a commercial location shared with hundreds of other merchants. Government registries may be highly digitized in one market and fragmented in another.

Applying the same evidentiary process everywhere does not necessarily create the same level of assurance.

It may simply create different levels of customer friction.

That requires the company to define the control objective first.

Are we establishing identity? Residential address? Business activity? Ownership? Source of funds? Authority to act?

Once the objective is clear, the company can approve locally credible evidence pathways that achieve the same global assurance standard.

This is more difficult than maintaining one checklist. It is also far more defensible, scalable and customer-centered.

When compliance requirements are converted into configurable product logic, the platform can collect the right evidence for the right customer in the right market—rather than sending everyone through a process designed for somewhere else.

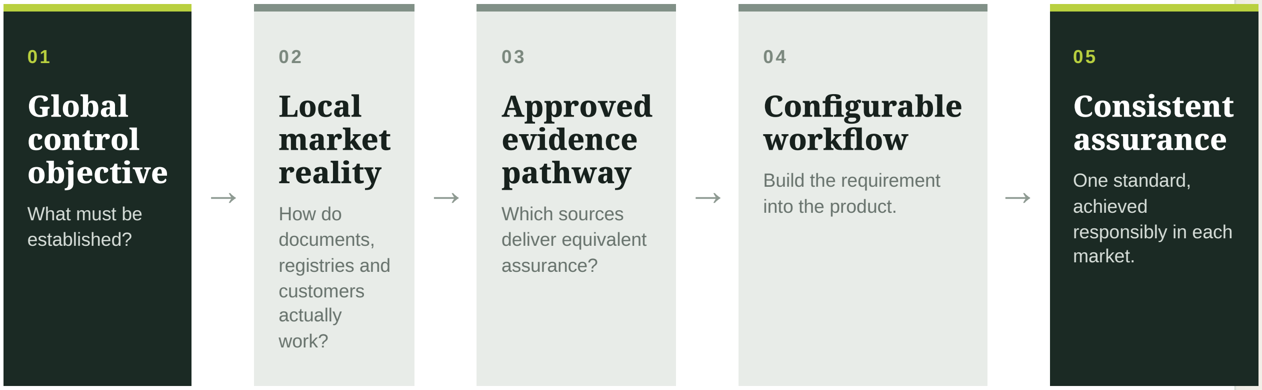
That is what compliance by design looks like.

> “ Standardize what the institution needs to know - not the exact artifact every customer must provide.

FIGURE 2

Global Standards, Local Reality

Standardize assurance. Localize the evidence and workflow used to achieve it.



01
Global control objective
What must be established?

→

02
Local market reality
How do documents, registries and customers actually work?

→

03
Approved evidence pathway
Which sources deliver equivalent assurance?

→

04
Configurable workflow
Build the requirement into the product.

→

05
Consistent assurance
One standard, achieved responsibly in each market.

05

FROM ALERTS TO UNDERSTANDING

Compliance as an Intelligence Function

Traditional compliance programmes were built around alerts.

A rule triggers. An analyst reviews. A case is closed or escalated.

But payments companies see much more than individual alerts.

They see identity, ownership, devices, geographies, payment counterparties, withdrawal behaviour, transaction velocity, account recovery attempts, network relationships and changes in customer activity.

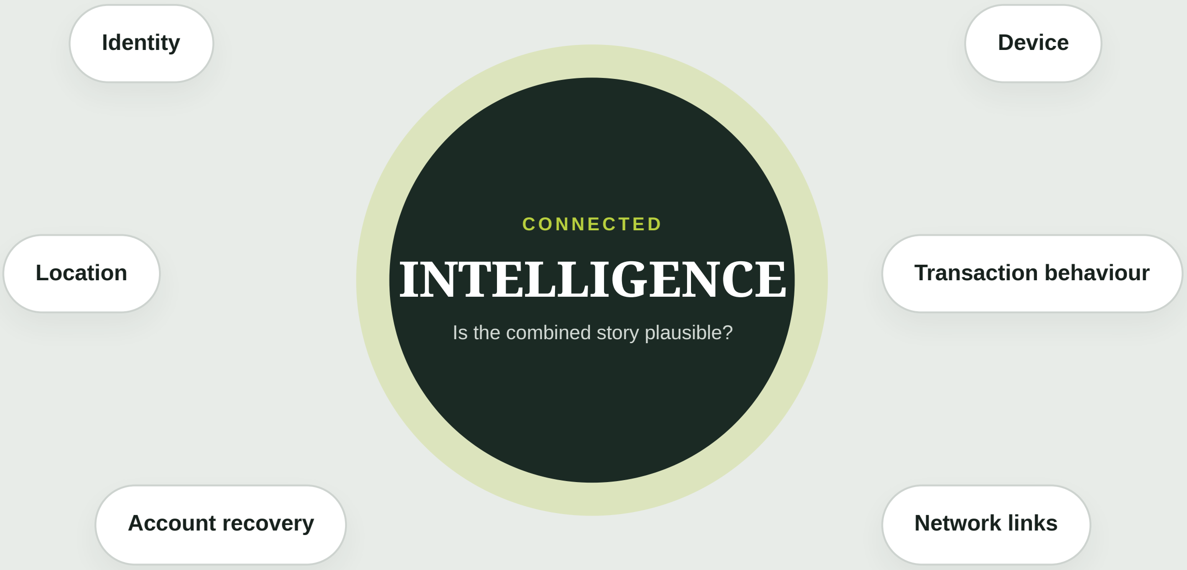
Taken separately, many of these signals may appear legitimate.

Together, they can reveal something entirely different.

FIGURE 3

From Signals to Intelligence

No single indicator proves illicit activity. Intelligence emerges from relationships, contradictions and cumulative context.



Consider a customer who declares that they are located in the United States. The account regularly logs in from Europe or Asia. The device language is Korean. Identity information appears Chinese. Password-reset activity is frequent. Withdrawals occur near the Chinese border with North Korea. Several apparently unrelated accounts share devices, beneficiaries or access patterns.

No single indicator proves illicit activity.

The intelligence lies in the relationship between them.

This is increasingly important because modern financial crime is designed to look legitimate.

The identity may be false, but the work is real. The company may be real. The transaction may be commercially plausible. The employer may receive the service it purchased.

Traditional screening may therefore find nothing.

The future of compliance depends on connecting individually plausible facts into an implausible whole.

This is where payments companies can develop a genuine intelligence advantage. Their position in the financial ecosystem gives them visibility across behaviour, identity and movement of funds that few other institutions possess.

The competitive question is whether that intelligence remains trapped inside alerts—or becomes available to product leaders, executives and risk owners early enough to influence decisions.

CASE STUDY · STATE-SPONSORED FINANCIAL CRIME

The Customer Who Does Not Exist

North Korean remote IT-worker networks demonstrate how quickly the threat environment has changed.

The traditional sanctions model assumes that an institution can identify a prohibited party through a name, location or listed entity.

But a state-sponsored worker may use a stolen or synthetic identity, access a legitimate employment or freelancer platform, complete genuine technical work and receive payment through apparently ordinary channels.

> The work is real. The code gets written. The tickets get closed. Only the identity is fake.

Detecting that activity requires far more than sanctions-list screening.

It requires identity intelligence, device analysis, geographical inconsistencies, account-recovery controls, network relationships and payment behaviour to be assessed together.

It also requires the institution to change its controls as the threat adapts.

For example, strengthening password recovery so that a user must provide both a live selfie and a physically held identity document does more than reduce account takeover. It also makes accounts more difficult to sell, transfer or operate remotely by an undisclosed third party.

This is an important distinction.

The strongest compliance controls do not simply detect abuse after it occurs.

They change the economics of abuse.

They make the platform harder to exploit than competing channels.

That is both a control outcome and a strategic advantage.

FIGURE 4

The transaction may look legitimate. The contradiction becomes visible only when identity, access and network behaviour are connected.

DECLARED PROFILE

Customer identity appears ordinary

- Claimed location
- Valid-looking identity documents
- Commercially plausible work

+

OBSERVED BEHAVIOUR

Signals do not align

- Login geography
- Device or language inconsistency
- Account-recovery anomalies
- Withdrawal geography
- Shared network links

=

INTELLIGENCE ASSESSMENT

Individually plausible. Collectively implausible.

Escalate for investigation without treating any single trait as proof.

CASE STUDY · GEOPOLITICAL RESILIENCE

Staying Open During a Crisis

Geopolitical crises reveal the difference between mature compliance and blunt risk avoidance.

When Russia invaded Ukraine, financial institutions faced an environment of rapidly changing sanctions, payment disruption, humanitarian concerns and significant uncertainty.

The simplest response would have been to withdraw broadly from the region.

But broad withdrawal can harm legitimate customers while doing little to distinguish between lawful activity and prohibited risk.

Institutions with strong local intelligence, capable sanctions teams, reliable data and clear governance have more options.

They can identify where customers are located, understand how restrictions apply, distinguish between sanctioned and legitimate activity, monitor payment patterns and adapt controls as the situation changes.

That capability does not eliminate risk.

It allows the institution to manage risk with greater precision.

For global payments companies, this matters commercially as well as ethically. The ability to continue serving legitimate customers during disruption can preserve trust, protect important markets and demonstrate to regulators and partners that the company can operate responsibly under pressure.

Compliance maturity creates alternatives.

Without it, the institution may be left with only two choices: ignore the risk or abandon the market.

FIGURE 5

Mature compliance creates options beyond ignoring risk or abandoning a market.

BLUNT RESPONSE

Retreat

- Broad withdrawal
- Overblocking
- Loss of legitimate customers
- Limited learning

Lower complexity, lower reach, weaker intelligence.

VS

ADAPTIVE RESPONSE

Precision

- Local intelligence
- Risk segmentation
- Sanctions precision
- Ongoing monitoring
- Legitimate customer continuity

More choices, stronger trust, controlled continuity.

06

OPERATING CAPABILITY

Technology Is Not the Advantage

Payments and fintech companies invest heavily in compliance technology.

They purchase screening systems, monitoring platforms, machine-learning models, identity tools and case-management systems. Increasingly, they are experimenting with generative AI and autonomous agents.

But two companies can buy the same technology and achieve completely different outcomes.

Technology does not create competitive advantage by itself.

Operating capability does.

A model can identify unusual behaviour, but the institution must decide what performance means; how drift will be detected; who can challenge the model; when thresholds can change; how outcomes are explained; which decisions require human judgment; how emerging threats are incorporated; and how the model is governed over time.

The same is true of sanctions screening, KYC automation and fraud detection.

The advantage belongs to the organization that can integrate technology into a coherent system of intelligence, governance and decision-making.

Without that system, technology simply automates existing weaknesses.

> “ Artificial intelligence can accelerate judgment. It cannot replace accountability.

FIGURE 6

Technology Is Not the Advantage

Two institutions can buy the same stack and achieve completely different outcomes.

Screening | **Monitoring** | **Identity** | **AI** | **Case management**

INSTITUTION A

Tools without operating capability

- Fragmented governance
- Late product involvement
- Periodic model challenge
- Automation of existing weaknesses

More technology. Same institutional friction.

INSTITUTION B

Integrated operating capability

- Clear ownership
- Compliance by design
- Continuous model oversight
- Human judgment and accountability

Better risk outcomes. Better customer outcomes.

07

ACCESS IS EARNED

Trust as Economic Infrastructure

Trust is often discussed as though it were intangible.

In payments, it produces measurable commercial effects.

A trusted company can complete due diligence more quickly. Banks are more willing to expand relationships. Regulators are more likely to believe that issues will be identified and addressed. Enterprise customers are more comfortable routing significant volume through the platform.

A trusted company is not one that claims to be perfect.

It is one that demonstrates awareness, responsiveness and control.

Partners want to know: Does the institution understand its risks? Can it explain how its systems work? Does it identify weaknesses before someone else does? Does it respond transparently? Can it adapt when the threat changes?

Trust grows through evidence.

That evidence includes governance records, model monitoring, consistent customer decisions, timely regulatory reporting, effective remediation and the willingness to acknowledge uncertainty.

The commercial value of trust becomes most visible during a crisis.

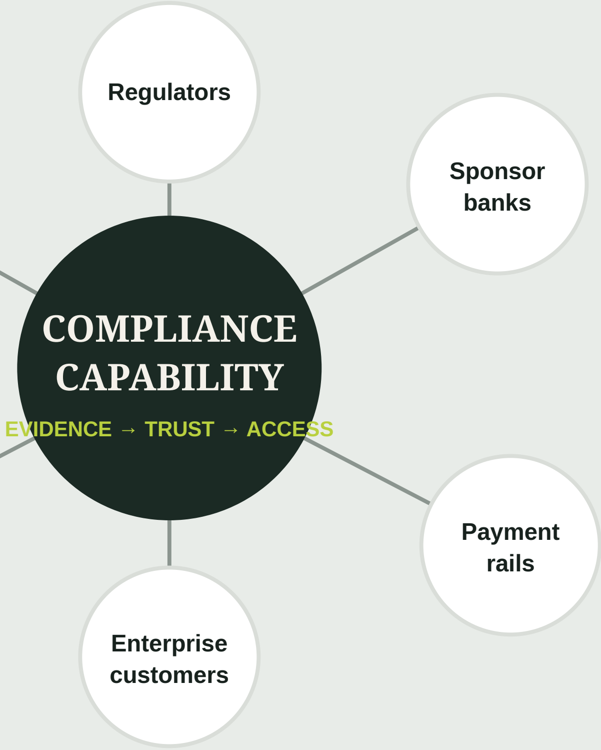
When a control failure occurs, a new threat emerges or a regulator raises concerns, institutions with strong credibility have more room to respond. Their partners may remain engaged because they believe the company can manage the problem.

Trust creates strategic resilience.

FIGURE 7

Trust Creates Access

In payments, trust determines access to the infrastructure on which growth depends.



08

GLOBAL STANDARDS, LOCAL INTELLIGENCE

The Global Operating Model

Global growth requires more than expanding a central compliance team.

It requires an operating model that combines consistent standards with local intelligence.

A mature global function needs central governance, specialist expertise, regional knowledge and continuous coverage. It must understand not only what a policy says, but how customers, documents, payment practices and regulatory expectations differ across markets.

Global hubs can provide resilience, access to talent and 24-hour operations. But globalization should not become a euphemism for labor arbitrage.

The real advantage comes from diversity of perspective and proximity to risk.

A team in one market may identify a documentation pattern that would appear unusual elsewhere but is entirely normal locally. Another may recognize a fraud typology, payment corridor or sanctions concern before it becomes visible globally.

The global compliance organization should function as a network of intelligence—not a central team issuing instructions to remote processing centers.

When structured properly, local teams improve global decision-making.

They allow the institution to move faster because it does not need to relearn each market from first principles.

FIGURE 8

Six Sources of Competitive Advantage

Compliance becomes commercial capability through six linked outcomes.

01

Market access

Earn the confidence required for licences, banks, rails and new markets.

02

Speed through certainty

Reach the best-supported decision earlier, with fewer late surprises.

03

Product and customer experience

Reduce unnecessary friction through intelligent, risk-based controls.

04

Trust infrastructure

Shorten diligence, deepen relationships and preserve access in a crisis.

05

Intelligence advantage

Turn payment, identity and network data into strategic insight.

06

Resilience

Adapt to disruption without abandoning legitimate customers or losing control.

09

THE BUSINESS SCORECARD

Measuring What Compliance Creates

The business value of compliance will remain disputed for as long as the function measures only activity.

Budgets, headcount, alert volumes, case turnaround and training completion may be useful operational measures. They do not show whether compliance is improving the company's ability to grow.

A more meaningful scorecard would measure five outcomes.

These measures do not replace traditional compliance metrics. They reveal whether the function is creating institutional capability—or simply processing work.

FIGURE 9

The Compliance Advantage Scorecard

Measure what the function enables - not only what it processes.

DIMENSION	REPRESENTATIVE MEASURES
Growth enablement	Time from commercial proposal to compliance decision; percentage of launches involving compliance during design; products and markets enabled through reusable controls; partner and bank due-diligence cycle time.
Customer experience	Onboarding conversion; manual-review rate; unnecessary document-request rate; false-positive customer interventions; time to resolve restrictions and appeals.
Risk intelligence	Time to identify emerging typologies; time from identified threat to implemented control; quality of risk data; network and cross-product detection capability.
Trust and access	Regulatory findings and repeat issues; partner escalations; licence outcomes; institutional due-diligence cycle time; quality and timeliness of regulatory engagement.
Adaptability	Time from regulatory change to implementation; model-drift detection and remediation; configurable controls; speed of response during geopolitical or criminal events.

> “ The fastest company is not the one that says yes the most. It is the one that can reach the best-supported decision the quickest.

10

LEADERSHIP

The Strategic CCO

The role of the Chief Compliance Officer is changing.

The traditional CCO was expected to interpret regulation, maintain policies, oversee investigations and prevent misconduct.

Those responsibilities remain.

But the strategic CCO must also understand products, technology, customer behavior, data, market expansion and commercial trade-offs.

The role is not to remove risk from the company.

No payments company can innovate or grow without taking risk.

The role is to help the company distinguish between risk it does not understand; risk it understands but cannot control; risk it can mitigate; risk it is prepared to accept; and opportunity disguised as complexity.

That requires judgment.

It also requires the confidence to say no when the risk cannot be supported—and the imagination to design a responsible path forward when it can.

The best compliance leaders do not ask only: Can we approve this?

They ask: What would need to be true for us to do this responsibly?

That is a fundamentally different posture.

It turns compliance from a gate at the end of the process into an architect at the beginning.

11

CLOSING ARGUMENT

The Company That Understands Risk First

Fintech has spent years celebrating speed.

Faster onboarding. Faster payments. Faster product development. Faster expansion.

But speed without understanding eventually creates fragility.

The companies most likely to win are not those that move first regardless of risk. They are those that understand risk early enough to move with confidence.

They will use compliance to design better products, localize customer journeys, strengthen partnerships, protect market access and respond to threats without unnecessary retreat.

They will treat compliance data as intelligence.

They will govern technology as a living system.

They will measure trust, adaptability and decision speed—not just alerts and cost.

And they will recognize that compliance is not simply the price of participating in financial services.

THE CLOSING PROPOSITION

In payments and fintech, compliance is part of the product, part of the infrastructure and - when built properly - a competitive advantage.

01 · PRODUCT

Designed into experience

Identity, monitoring, restrictions and appeals shape conversion, trust and customer outcomes.

02 · INFRASTRUCTURE

Access depends on it

Licences, banks, payment rails and enterprise relationships depend on confidence in control.

03 · ADVANTAGE

Understanding creates speed

Earlier intelligence enables better decisions, stronger trust and greater strategic freedom.

The companies that understand risk first are the companies best positioned to move with confidence.

EXECUTIVE REFLECTION

Questions for Leaders

01 Does compliance become involved while products are being designed, or when approval is already expected?

02 Can the company explain how its compliance programme enables growth—not only how it prevents loss?

03 Are customer controls localized to achieve consistent assurance, or simply standardized for internal convenience?

04 Does compliance intelligence influence product and market decisions?

05 Can the institution adapt controls faster than the threats it faces?

06 Would banks, regulators and customers describe compliance as one of the reasons they trust the company?

The answer to these questions may reveal more about a payments company’s future than its product roadmap.

MS

About Micheal Sheehy

Micheal Sheehy is a global compliance executive focused on the intersection of payments, financial crime risk, technology and organizational design. His work centers on building scalable compliance programmes, modernizing customer and transaction controls, and helping international businesses grow with confidence across complex regulatory environments.

Contact: michealsheehy@gmail.com · **Website:** michealsheehy.com

ADAPTIVE COMPLIANCE · EXECUTIVE ESSAY

MS

The companies that move fastest are not those that ignore risk. **They are those that understand it earliest.**

Compliance as a Competitive Advantage in Payments and Fintech

---

michealsheehy.com · michealsheehy@gmail.com