GCC Payments M&A: Diligencing Take Rate, Float, Compliance and Merchant Concentration

A Transaction Framework for Revenue Quality, Safeguarded Funds, Merchant Cohorts, Regulatory Perimeter and Integration Value

Authored by Chennakeshav Adya, Independent Researcher

September 2026

Abstract

Payments businesses can show rapid transaction growth while economic value depends on a narrower set of variables: the price retained after pass-through costs, merchant retention, mix, fraud and credit losses, settlement discipline, compliance capability and the legal right to provide each service. These variables are especially important in Gulf Cooperation Council markets, where local licensing, domestic payment infrastructure, cross-border flows, merchant digitisation and platform partnerships can create both growth and execution complexity.

This paper develops a transaction framework for acquiring, investing in or combining a GCC payments business. It traces a payment from merchant acceptance through authorisation, clearing, settlement and payout; rebuilds the reported take rate into an auditable revenue and contribution bridge; distinguishes operational settlement balances from freely available corporate cash; measures merchant cohorts and concentration; and converts regulatory, compliance, technology and commercial findings into valuation, contractual protection and a 100-day plan. Five original figures and five implementation tables provide a practical architecture for diligence and post-close execution.

Public evidence illustrates the scale and operating importance of payment systems without establishing the quality of any target. The Central Bank of the UAE reported that its Instant Payment Instruction platform, including Aani, processed 33.8 million transactions with a value of AED 168.8 billion during 2025.[6] The Saudi Central Bank reported that electronic payments represented 85 per cent of retail payments in Saudi Arabia during 2025, with 14.6 billion electronic transactions compared with 12.6 billion in 2024.[12] These system-level measures should not be used as substitutes for target-level merchant, revenue, settlement or compliance evidence.

Every balance, rate, cohort, margin, concentration, haircut, probability, cash flow, valuation effect and transaction outcome in this paper is a hypothetical analytical assumption used to demonstrate the framework. It is not a forecast, market quotation, investment recommendation, legal conclusion, accounting conclusion, regulatory conclusion or fairness opinion. An actual transaction requires verified source records and qualified advice across corporate finance, law, regulation, accounting, tax, technology, cybersecurity, data protection, competition and financial crime.

JEL Classification: G21, G24, G28, G34, L86

Keywords: GCC payments, payments M&A, merchant acquiring, take rate, settlement float, safeguarded funds, merchant concentration, compliance diligence, revenue quality, fintech valuation

1. Begin with the payment and the cash it creates

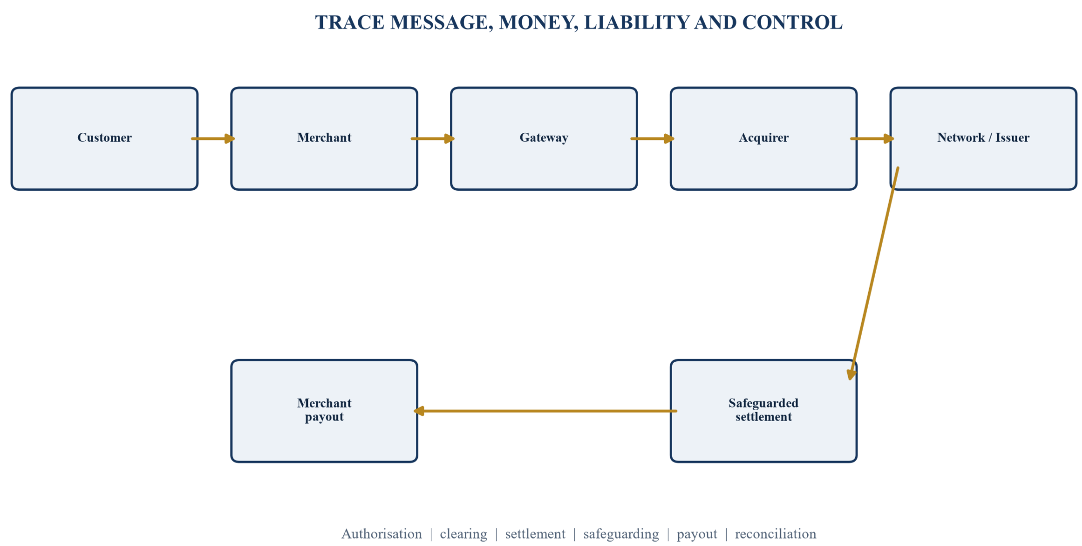
A payments target can describe itself through total payment volume, processed transactions, active merchants or geographic reach. None of those measures alone establishes revenue quality or cash generation. The transaction team should begin with a traceable payment and identify the legal entities, systems, counterparties, accounts, fees, liabilities and timing at each step from customer initiation to final merchant payout.

The evidence chain should connect merchant contract, transaction message, gateway record, processor record, scheme or network file, acquiring record, settlement statement, bank receipt, merchant payout and general ledger. Transaction identifiers and timestamps should permit sampling across this chain. Differences in timezone, batch cut-off, currency conversion, refunds, chargebacks and delayed settlement need explicit rules so that the bridge can be reproduced.

The buyer should distinguish services that the target performs from services sourced from a sponsor bank, processor, scheme, wallet, fraud vendor or payout partner. A target may own the merchant relationship while relying on third parties for regulated processing and settlement. Another target may hold a licence and operate the acquiring stack while outsourcing selected technology. These models have different margin, control, continuity and change-of-control implications.

The first diligence output should be a payment value-chain map supported by sample transactions and account reconciliations. It becomes the organising document for commercial, financial, regulatory, technology and operational workstreams.

Figure 1. Illustrative payment value chain and cash-rights map



The diagram is a diligence framework. Legal rights and settlement paths must be verified for each target, service and jurisdiction.

2. Define the legal entity, licence and service perimeter

Payments groups frequently operate through several legal entities, licences and commercial arrangements. The buyer should identify which entity contracts with each merchant, performs each regulated activity, holds or controls funds, employs critical staff, owns software and data, and records revenue. Group presentations can obscure a licence dependency or a material intercompany service that will change after closing.

The UAE Retail Payment Services and Card Schemes Regulation identifies nine categories of retail payment service, including merchant acquiring, payment aggregation, payment account issuance, payment instrument issuance, payment initiation and payment account information services.[1] The buyer should map the target's actual activities to the applicable category and verify the licence, exemptions, conditions, territorial scope and regulatory correspondence. The Saudi Payments and Payment Services Law and its implementing regulations require a separate jurisdiction-specific assessment.[8][9]

Change of control may require approval or notification. A transaction timetable should therefore integrate regulatory engagement, ownership disclosure, controller fitness, capital, governance, systems, outsourcing and local substance. Signing conditions should reflect the evidence and authority required before control passes. The buyer should also assess whether the proposed operating model after integration remains within the approved perimeter.

The legal-perimeter work should end with an entity-by-service matrix. Any revenue attributed to an entity without the necessary right, contract or operational capacity should be isolated until resolved.

Table 1. Legal, licence and operating-perimeter evidence map

Perimeter item	Primary evidence	Transaction question	Deal response
regulated activity	licences, regulatory registers, legal advice and correspondence	which entity may perform each service and in which market?	approval condition, perimeter representation and remediation
merchant relationship	contracts, onboarding files, pricing schedules and novations	who owns the contract and may it transfer on control?	consent plan, retention condition and value adjustment
settlement responsibility	account mandates, safeguarding terms and bank confirmations	who owes the merchant and who controls funds?	cash covenant, account control and closing reconciliation
technology and data	ownership records, licences, hosting contracts and data maps	can the buyer operate and migrate the stack lawfully?	IP condition, transitional service and migration plan
outsourced dependency	sponsor, processor, scheme and vendor agreements	can a counterparty terminate, reprice or restrict the business?	waiver, replacement readiness and dependency reserve

Exact permissions, approvals and evidence depend on the service, entity and jurisdiction.

3. Build an auditable transaction-level data set

The diligence data set should start with transaction records at the finest useful level. Core fields include merchant, legal entity, outlet, channel, geography, currency, payment method, authorisation result, gross amount, refund, chargeback, settlement date, merchant payout, gross merchant fee, interchange or issuer cost, scheme fee, processor cost, foreign-exchange component, incentive and net revenue. Stable identifiers should link the records to contracts, settlement statements and accounting entries.

Field definitions need owners, system sources, refresh frequency, validation rules and change history. Gross payment volume may include or exclude refunds, reversals, cash withdrawals, money movement, marketplace sub-merchants or non-card methods. Active merchant can mean one transaction in a period or a minimum level of activity. The buyer should restate metrics using a documented definition and preserve the management definition for reconciliation.

Data tests should address duplicates, missing identifiers, impossible chronology, negative values, currency conversion, outliers and unexplained mapping changes. Monthly totals should reconcile to operational reports, bank accounts, revenue records and statutory accounts. Acquired portfolios and system migrations should be tagged so that apparent organic growth is not created by a perimeter change.

Personal and cardholder data should be minimised for transaction diligence. Tokenised or aggregated records can support most analysis. Access, encryption, retention, permitted use and deletion should be documented with legal and security teams.

4. Rebuild the take rate from contract to ledger

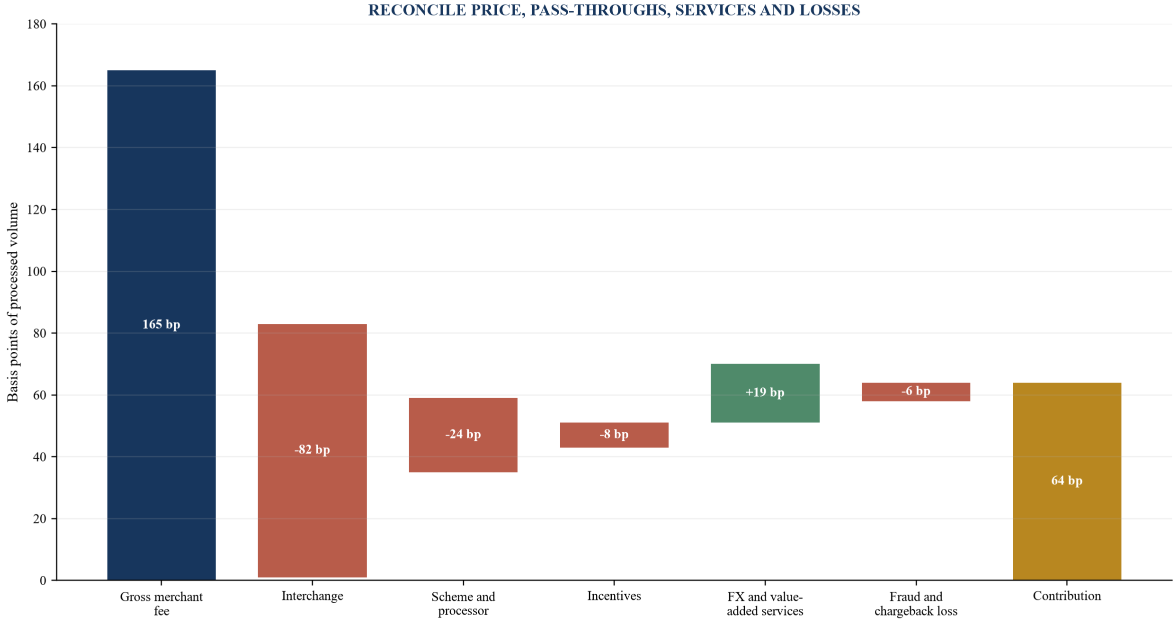
Headline take rate is commonly calculated as revenue divided by payment volume. Its meaning depends on which revenue and which volume are used. A gross merchant service charge can include interchange, scheme and processor amounts that pass through to other parties. Net revenue may include foreign-exchange, gateway subscriptions, device rental, fraud tools, lending referrals or other services that do not scale directly with payment volume.

The buyer should build a monthly take-rate bridge from contract pricing and transaction data. It should distinguish gross merchant fees, pass-through costs, rebates, incentives, refunds, chargeback fees, cross-border and currency income, value-added services, accounting adjustments and direct loss. Each component should be reported in basis points of the relevant volume and in absolute currency.

IFRS 15 requires revenue recognition based on the nature of the performance obligation and includes a principal-versus-agent assessment when another party participates in providing goods or services.[16][17] The diligence team should review accounting policy, contracts and actual control over services. A presentation change between gross and net revenue can materially alter reported growth and margins without changing cash economics.

Take-rate quality should be measured by merchant cohort, channel, sector, payment method, country, contract vintage and contribution margin. A stable blended rate can hide declining prices in core merchants offset by volatile foreign-exchange or ancillary income.

Figure 2. Illustrative take-rate waterfall from merchant fee to contribution



Basis-point values are hypothetical analytical assumptions and do not describe a target or market quotation.

5. Separate volume growth from mix and price

Payment volume can grow through existing merchants, new merchants, acquisitions, a new method, geographic expansion, inflation, currency movement or a small number of large accounts. A buyer should decompose growth before applying a multiple. Existing-merchant growth often has different retention and acquisition economics from newly boarded volume.

The analysis should present constant-currency volume and revenue where multiple currencies are material. It should separate domestic, cross-border and foreign-exchange-enabled transactions because pricing, cost and regulatory treatment differ. Channel migration from point of sale to e-commerce can change fraud, scheme cost and merchant expectations. Debit, credit, wallet, account-to-account and alternative methods can carry different unit economics.

Public company disclosures illustrate why metric definitions matter. Adyen reported more than EUR 1 trillion of global payment transactions processed in 2024 and described net revenue as a central financial measure.[18] Block reported 2024 total gross payment volume of USD 240.8 billion across Square and Cash App.[20] These are company-defined measures from different business models and should not be treated as directly comparable benchmarks for a GCC target.

A volume bridge should tie opening merchants and volume to expansion, contraction, churn, new wins, acquisitions and currency. The corresponding revenue and contribution bridge should use the same cohorts. This reveals whether growth creates distributable economics or only operational scale.

6. Reconcile revenue to settled cash

Revenue quality requires evidence from transaction through invoice, settlement and cash. The buyer should reconcile recognised revenue to gross merchant fees, third-party deductions, merchant payouts, receivables, deferred amounts and bank receipts. Timing differences should be explained by cut-offs, reserve holds, refunds, disputes, billing cycles or accounting policy.

The cash bridge should distinguish money collected on behalf of merchants from the target's own fee income. A large cash balance can arise because merchant settlement has not yet occurred. It may be restricted, safeguarded or operationally committed. Counting that balance as available corporate cash can overstate net cash and enterprise value.

Unbilled or accrued revenue should be tested against contracts and subsequent settlement. Manual journals, suspense accounts and aged reconciliations deserve targeted review. A rapid rise in revenue receivables relative to volume may indicate billing problems, merchant disputes, weaker counterparties or a change in recognition. Incentives and rebates should be accrued in the same periods as the related activity.

The transaction model should use verified free cash generation after merchant obligations, direct network and processor costs, losses, working capital, capital expenditure, regulatory capital and necessary technology investment.

7. Map settlement float and ownership of funds

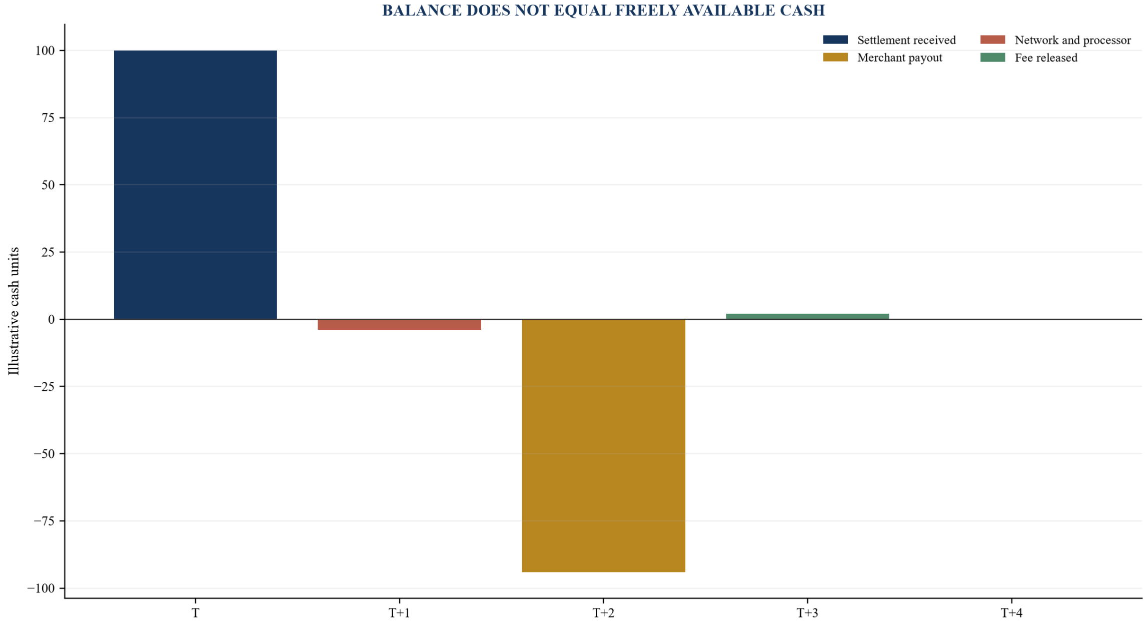
Settlement float describes balances and timing between receipt from payment participants and payout to merchants or users. The economic and legal character of those balances varies. Some funds may be held for users under safeguarding requirements; some may be due to merchants under contract; some may represent reserves or chargeback cover; and a limited portion may be the target's earned fee.

The UAE regulation requires licensed payment service providers to safeguard user funds through prescribed arrangements, including segregation and reconciliation obligations.[4] The buyer should verify account titles, bank acknowledgements, trust or safeguarding terms, investment permissions, reconciliation frequency, breach history and the treatment of interest. The Saudi framework requires a separate assessment of safeguarding and settlement obligations.[8][9]

Float analysis should cover gross balance, legal owner, beneficial claimant, currency, bank, country, ageing, expected payout, reserve, lien, interest, counterparty exposure and liquidity accessibility. Weekend and holiday peaks should be tested. A merchant payout delay can temporarily increase bank balances while creating an equal or larger liability and reputational risk.

Transaction documents should define which cash is delivered at closing, how restricted and merchant balances are treated, and how leakage between signing and closing is prevented. The buyer may require a specific closing reconciliation and a minimum liquidity buffer.

Figure 3. Illustrative settlement float and liquidity timeline



Timing and amounts are hypothetical analytical assumptions. Actual settlement terms must be verified by method, merchant and counterparty.

8. Test safeguarding and bank-counterparty exposure

Safeguarding is both a regulatory obligation and an operational control. The buyer should inspect daily or more frequent reconciliations between transaction liabilities, merchant or user sub-ledgers and bank balances. Unreconciled items should be aged, assigned and resolved. System-generated reconciliations require sample testing of source completeness and logic.

Bank exposure can be concentrated even where merchant exposure is diversified. The analysis should show balance by bank, account, currency, legal regime, credit quality, access right and intraday peak. A bank failure, account freeze, sanctions issue or operational outage can interrupt payout. Diversification, sweep rules and contingency accounts should be tested under realistic transfer timelines.

The buyer should review whether interest or other economic benefit on safeguarded funds may be retained and how it is recognised. The legal answer can differ by contract, regulation and jurisdiction. A valuation should avoid capitalising float income that depends on rising rates, extended settlement or use of funds that is restricted.

Historical breaches, late payouts, negative safeguarding positions, manual top-ups and regulator correspondence should enter the risk assessment. Remediation should identify cash needed, system changes, governance and assurance. A closing condition may be appropriate where the shortfall or control weakness is material.

Table 2. Settlement-float and safeguarding reconciliation

Test	Evidence	Failure signal	Transaction response
liability completeness	merchant and user sub-ledgers, scheme files and cut-off reports	bank balance reconciles only after omitted liabilities	independent recalculation and closing adjustment
segregation	account titles, mandates, bank letters and legal opinions	corporate payments pass through safeguarded accounts	account redesign, covenant and remediation reserve
timeliness	daily reconciliations, exception logs and payout reports	aged breaks or repeated manual top-ups	root-cause plan and enhanced monitoring
counterparty exposure	bank balances, limits, ratings and contingency plans	single-bank or single-country dependency	diversification plan and liquidity buffer
interest and access	contracts, regulation, accounting policy and approvals	income assumes unrestricted use or delayed payout	valuation exclusion and legal confirmation

Balances and thresholds should be defined using the target's verified legal and operational model.

9. Measure merchant cohorts, retention and expansion

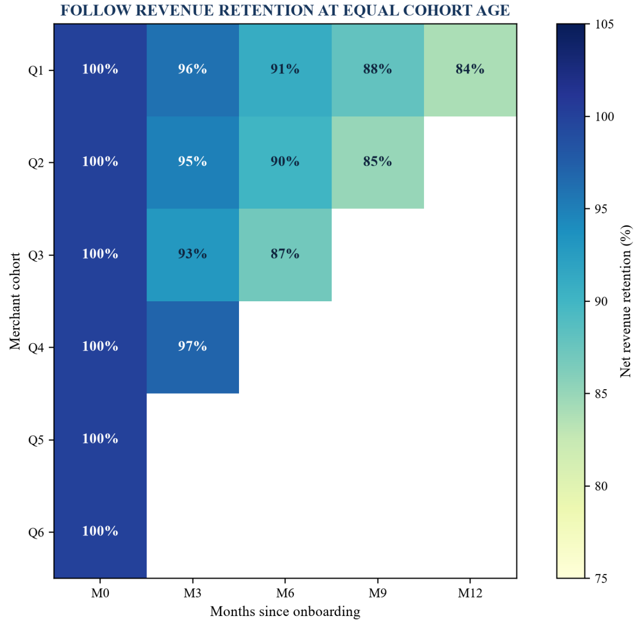
A merchant count can rise while the economically valuable base weakens. Cohort analysis groups merchants by onboarding period and tracks payment volume, net revenue, contribution, product use and activity over equal periods. It should distinguish logo retention from volume retention and revenue retention.

Merchant churn requires a consistent definition. Seasonal merchants, low-frequency professional services, dormant accounts, portfolio transfers and entity changes can be misclassified. The buyer should define inactivity windows by segment and test reactivation. Cohorts should be split by sector, channel, country, size, sales source, pricing plan, integration type and sponsor relationship.

Expansion can come from merchant sales growth, share-of-wallet gain, additional locations, new methods, cross-border use or value-added services. These drivers have different durability. Contraction can signal merchant distress, competitive switching, operational failure or lower consumer demand. The commercial team should validate reasons using contracts, service records and merchant interviews under an approved protocol.

The valuation model should connect cohort retention to acquisition cost and contribution. A business that replaces lost merchants through heavy incentives may show volume growth while destroying lifetime value.

Figure 4. Illustrative merchant revenue-retention cohorts



Retention rates are hypothetical analytical assumptions and do not describe a target.

10. Quantify merchant concentration beyond the top ten

Top-ten concentration is a useful starting point and an incomplete risk measure. A buyer should calculate concentration by payment volume, net revenue, contribution, receivable, settlement liability and loss. A large low-margin merchant can create operational and counterparty exposure while contributing little value. A smaller merchant with high foreign-exchange or value-added-service revenue can have disproportionate profit importance.

Concentration should also be measured by corporate group, platform, sponsor bank, software integration, sector, country, channel and sales partner. Multiple merchant IDs can belong to one economic group. Marketplace sub-merchants can create indirect concentration. A shared e-commerce platform, airline sector or government contract can produce correlated volume changes.

Contract terms matter. The buyer should record expiry, termination, change-of-control, minimum volume, exclusivity, pricing review, reserve, liability, data use and service level. Concentrated merchants with short termination rights or bespoke technology should receive a different valuation treatment from diversified merchants under durable contracts.

The deal model can apply retention scenarios by cohort and merchant group, with contribution rather than volume as the base. Closing conditions, earn-outs, escrow or purchase-price adjustment may address material dependency where the seller cannot deliver acceptable consent or retention evidence.

11. Test merchant unit economics and acquisition payback

Merchant-level contribution should deduct variable network, processor, device, fraud, chargeback, support, settlement, incentive and sales-channel costs from net revenue. Shared technology and compliance costs can then be allocated for segment analysis. The purpose is to understand which relationships fund the platform and which depend on scale or future repricing.

Customer acquisition cost should include sales payroll, commissions, partner fees, onboarding, underwriting, device subsidy, integration support and promotional pricing. Payback begins when cumulative contribution covers those costs. A reported payback that ignores sales-channel commission or hardware replacement can be misleading.

The buyer should compare cohorts acquired through direct sales, banks, platforms, independent sales organisations and digital channels. Partner-sourced merchants may be cheaper to acquire but subject to revenue share or termination risk. Enterprise merchants may require long implementation and procurement cycles. Small merchants may onboard quickly but demand hardware, support and field coverage.

Unit economics should be stress-tested for price compression, scheme-cost increase, fraud, slower growth and churn. The valuation should credit growth where the evidence shows repeatable acquisition, retention and contribution after the full cost to serve.

12. Diligence fraud, chargebacks and merchant credit

Fraud and chargeback exposure can sit with issuer, acquirer, processor or merchant depending on method, authentication, scheme rules and contract. The buyer should measure gross fraud, net loss, recovery, chargeback, representment success, reserve and operational cost by merchant, sector, country, channel and reason code.

Card-not-present, cross-border, recurring, high-ticket and delayed-delivery sectors can show different risk. Merchant insolvency can create future-delivery claims after volume has ceased. Airlines, travel, events, subscriptions and marketplaces may need sector-specific reserves based on delivery profile and refund rights. Fast merchant growth should be checked for transaction laundering, synthetic activity or weak underwriting.

Adyen stated that its 2026 fraud report used 2025 platform data representing approximately USD 1.6 trillion in processed global payment volume and described growing first-party fraud risk.[19] This disclosure provides context for the scale and evolution of fraud analysis; it does not establish loss rates for a GCC target. Target evidence should come from its own transaction, rule, case and recovery records.

The buyer should test rule performance, model governance, manual review, false positives, authentication, merchant monitoring, reserve setting and incident escalation. Loss should be measured on the cohort that generated it, including delayed claims.

13. Treat AML/CFT and sanctions as transaction economics

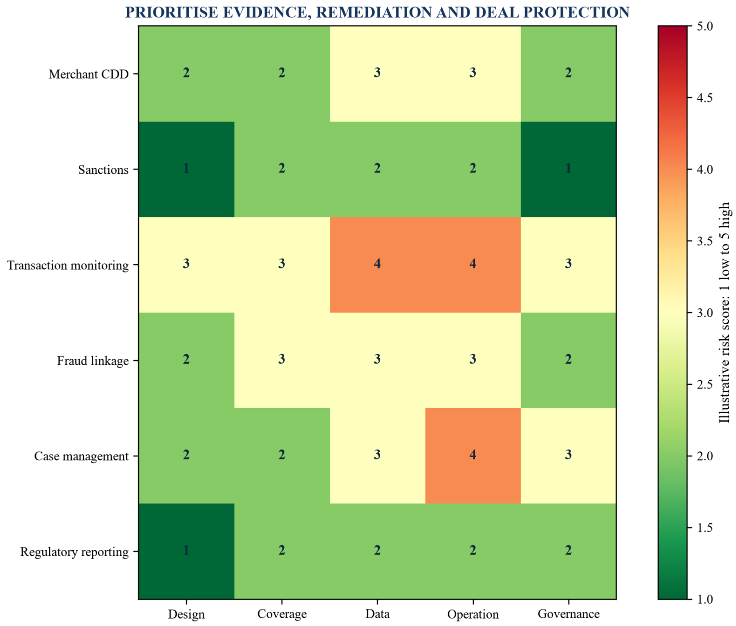
Payment businesses connect merchants, consumers, banks, networks and jurisdictions. Weak customer due diligence, merchant monitoring or sanctions screening can lead to remediation expense, merchant loss, settlement interruption and regulatory action. The diligence team should evaluate control design and its operation using source records rather than policy documents alone.

FATF's Recommendations provide the international framework for customer due diligence, beneficial ownership, suspicious transaction reporting, targeted financial sanctions and risk-based controls.[13] UAE licensed payment service providers must comply with applicable AML/CFT obligations and assess the risks associated with their services.[1][5] The buyer should map local requirements and supervisory expectations with qualified counsel.

The review should cover enterprise risk assessment, merchant onboarding, beneficial ownership, prohibited and restricted sectors, geographic risk, sanctions and politically exposed persons, transaction monitoring, investigations, reporting, quality assurance, training and governance. Samples should include high-risk, declined, exited and rapidly growing merchants. Backlogs, override rates, alert ageing and repeat findings should be quantified.

Remediation needs a costed plan with accountable owners, technology dependencies, data requirements and regulator engagement. A buyer should distinguish a documentation gap from a systemic failure that affects the right to operate. Deal protections may include conditions, specific indemnities, escrow, retention, covenants and a reduced valuation.

Figure 5. Illustrative compliance heat map for payments diligence



Scores are hypothetical analytical assumptions used to show prioritisation. They are not findings about a named business.

14. Review payment security and card-data scope

Security diligence should begin with the systems and data that support authorisation, routing, tokenisation, settlement, merchant administration and reporting. The buyer should map cardholder data, authentication credentials, cryptographic keys, personal data and privileged access across internal systems and vendors.

PCI DSS provides a baseline of technical and operational requirements for protecting payment account data.[21] Evidence should include the applicable assessment, scope, compensating controls, penetration testing, vulnerability management, segmentation and remediation. Certification status should be verified with the assessor and underlying reports. A valid attestation does not replace buyer testing of scope or control operation.

EMVCo's payment tokenisation framework helps explain how tokens can reduce exposure of primary account numbers within payment ecosystems.[22] The buyer should identify who operates the token vault, owns token relationships and supports lifecycle events. Tokenisation can reduce selected risks while creating dependency on token services, keys and integrations.

Incident records should be reconciled across security operations, fraud, customer support, insurers, vendors and regulatory notices. The transaction plan should price required upgrades, insurance, contractual liability, data migration and integration security. Critical remediation can be a closing condition where exposure cannot be contained after control passes.

15. Test platform reliability and operational resilience

Payment revenue depends on availability, latency, authorisation performance, accurate routing, settlement and payout. Service-level averages can obscure short failures during peak periods or concentrated merchant impact. The buyer should analyse event-level availability by component, method, geography and merchant, with timestamps and customer consequences.

The operating architecture should identify single points of failure across cloud regions, data centres, telecoms, banks, processors, networks, DNS, identity, keys and critical staff. Recovery objectives should be compared with demonstrated recovery from tests and incidents. Business continuity plans should include settlement and reconciliation, not only front-end processing.

Incident management evidence should show detection, triage, communication, containment, recovery, root cause and corrective action. Repeated similar incidents can indicate weak problem management. Change-failure rates, rollback capability, release governance and capacity testing are relevant to both current resilience and integration risk.

The buyer should quantify revenue credits, merchant claims, lost volume, manual workload and reputational impact. A 100-day plan can sequence monitoring, redundancy, vendor changes and architecture integration while protecting live payment flows.

16. Diligence third-party, scheme and sponsor dependencies

A payments business may rely on card schemes, domestic rails, sponsor banks, processors, token services, fraud vendors, cloud providers, device suppliers, telecoms and payout banks. The buyer should maintain a dependency register that links each service to merchants, volume, revenue, data, licences and recovery alternatives.

Contracts should be reviewed for change of control, termination, pricing, volume commitments, liability, audit, data location, subcontracting, exclusivity and transition. The buyer should test whether the target complies with scheme and sponsor requirements and whether any waiver is informal. Concentration should be measured by volume and contribution exposed to each dependency.

Operational substitutability should be demonstrated. A second vendor on paper may not have live capacity, certifications or merchant configuration. Migration can require merchant consent, device replacement, token portability, certification and regulator approval. Estimated replacement cost and time should enter the transaction case.

Key dependencies can be addressed through consents, new agreements, transitional services, redundancy investment and specific closing conditions. The integration plan should avoid changing several critical rails simultaneously.

17. Assess competition and economic-concentration approvals

Payments transactions can combine merchant networks, data, technology, distribution and regulated capabilities. Competition analysis should begin with relevant services and geographies rather than a single broad fintech label. Merchant acquiring, gateway, aggregation, wallet, processing and account-to-account services may have different competitors and switching conditions.

The UAE economic-concentration framework includes filing thresholds based on relevant-market sales and transaction share. Cabinet Decision No. 3 of 2025 identifies AED 300 million of relevant-market sales in the UAE or a transaction share above 40 per cent, subject to the statutory framework and applicable analysis.[14][15] Saudi Arabia has separate economic-concentration review guidelines issued by the General Authority for Competition.[10]

The transaction team should calculate thresholds using verified group revenue and market data, document methodology and engage counsel. The analysis may need to consider two-sided markets, merchant multi-homing, consumer access, data, interoperability, vertical relationships and potential foreclosure. Filing timing should be built into the critical path.

An uncertain competition timetable can affect financing, long-stop dates and integration planning. Clean-team protocols may be needed for merchant pricing, pipeline and other competitively sensitive information before approval.

18. Build a defensible quality-of-revenue bridge

Quality of revenue connects reported income to repeatable merchant economics. The buyer should begin with audited or reviewed accounts and bridge to transaction-level net revenue. The bridge should identify acquisitions, discontinued services, one-time fees, related parties, principal-agent presentation, foreign exchange, incentives, manual journals, unbilled amounts and prior-period corrections.

Recurring revenue should be defined by evidence. Transaction revenue can recur where merchant activity and retention are durable, even though it is usage-based. Contracted subscription revenue can be weak where merchants may cancel easily or service is not used. The analysis should show contractual status, cohort behaviour and contribution.

A monthly bridge should link volume, gross pricing, mix, pass-through cost, value-added services, loss and net revenue. The same bridge should be produced by top merchant, sector, country, channel and cohort. Variance from contract should be explained by negotiated pricing, routing, refunds, taxes, currency or data errors.

The output should support both valuation and purchase-price mechanics. It can define the revenue base for an earn-out, identify normalised working capital and separate merchant funds from corporate cash.

Table 3. Revenue and take-rate data dictionary

Measure	Required definition	Reconciliation	Diligence use
processed volume	authorised or settled, gross or net of refunds, currency rule	scheme, processor and settlement files	scale, mix and cohort growth
gross merchant fee	contractual and actual charge by transaction	merchant invoice and ledger	price realisation
pass-through cost	interchange, scheme, processor and partner amounts	third-party statements and cash	net take rate
value-added revenue	FX, fraud, devices, gateway, data and other services	contract, usage and invoice	durability and cross-sell
loss and incentive	fraud, chargeback, reserve, rebate and sales support	case records, contracts and ledger	contribution and payback

Definitions should be reconciled to contracts, transaction systems, settlements and the general ledger.

19. Convert findings into valuation scenarios

Payments valuation should be linked to revenue quality, contribution, merchant durability, regulatory capability and investment needs. A multiple applied to gross payment volume or gross revenue can ignore pass-through economics. The transaction model should use a measure that reflects the target's actual business model and reconcile it to cash.

The base case can begin with merchant cohorts, volume, take rate and contribution. Downside cases should test concentrated merchant loss, price compression, higher scheme or processor costs, fraud, delayed settlement, compliance remediation, technology investment and vendor repricing. Upside should require evidence such as signed merchant pipeline, demonstrated product adoption or achievable routing efficiency.

Restricted cash, safeguarded funds, merchant liabilities, reserves and regulatory capital should be treated separately from freely available cash and debt. Normalised working capital should reflect settlement cycles and seasonal peaks. Potential liabilities from chargebacks, disputes, compliance and tax require issue-specific analysis.

Transaction structure can allocate selected uncertainty through holdback, escrow, earn-out, warranty, indemnity or contingent value. The mechanism should rely on metrics that can be measured consistently after integration and should avoid incentives that damage compliance or merchant service.

20. Design transaction protections around identified risks

Representations and warranties should reflect the actual payment model. Relevant areas include licences, merchant contracts, settlement and safeguarding, financial crime, sanctions, scheme compliance, data security, processing accuracy, intellectual property, outages, complaints, reserves and related parties. Disclosure should be tested against diligence findings and regulatory correspondence.

Conditions precedent can address regulatory and competition approvals, sponsor or scheme consent, material merchant consent, safeguarding shortfall, security remediation and delivery of closing reconciliations. Covenants between signing and closing should preserve merchant service, liquidity, controls, key staff and ordinary-course pricing.

Specific indemnities or escrow may address known exposures that cannot be priced reliably. General warranty protection should not be expected to replace evidence or remediation. Limits, survival, knowledge and recovery mechanics need legal advice and negotiation.

The buyer should also protect the operating business. Overly broad restrictions can delay merchant decisions and product releases. The deal team should identify actions requiring consent and create a fast governance route during the interim period.

21. Plan integration around uninterrupted settlement

Integration success begins with a principle: merchants and users should continue to authorise, settle and receive payouts accurately. The buyer should map changes to legal entity, bank account, routing, merchant contract, brand, technology, support, finance, compliance and reporting. Each change requires a dependency, test and fallback.

Day-one activity should focus on governance, incident escalation, liquidity, access, regulatory commitments and critical counterparties. Technology consolidation can follow after transaction and settlement baselines are stable. Merchant migrations should be segmented by integration complexity and contractual consent.

Reconciliation should be strengthened during change. Parallel runs, control totals, exception thresholds and independent sign-off can reduce the risk of financial leakage. Data migration should preserve transaction history, chargeback evidence, merchant due diligence, complaints and regulatory records.

The integration model should measure value capture without weakening controls. Procurement savings, routing optimisation, platform consolidation and cross-sell should be net of migration cost, merchant attrition and operational risk.

22. Retain critical people and decision rights

Payments capability often depends on named individuals across regulation, treasury, settlement, risk, engineering, scheme relationships, merchant sales and incident management. The buyer should identify roles, authority, succession, contractual terms, location, workload and retention risk. A broad employee list does not reveal single-person dependencies.

Decision rights should be mapped for merchant approval, pricing exceptions, reserve release, sanctions escalation, settlement funding, system change and incident communication. Informal authority can create a gap when a founder or senior executive leaves. The integration design should allocate accountability before closing.

Retention arrangements should support continuity and knowledge transfer. Compensation should avoid incentives based solely on volume or revenue where risk quality matters. Objectives can combine merchant retention, control remediation, reliability, integration and contribution.

The 100-day plan should include succession for regulated and key-person roles, updated delegations, training and documented procedures. Material departures should trigger a review of operating capacity and transaction assumptions.

23. Establish post-close controls and management information

Post-close reporting should connect payment operations to financial and risk outcomes. A concise dashboard can cover processed and settled volume, net take rate, contribution, merchant cohorts, concentration, authorisation, fraud, chargebacks, settlement breaks, safeguarding, compliance alerts, outages and liquidity.

Metric ownership and definitions should be fixed before the first report. Changes to perimeter, mapping or methodology require approval and restatement where material. Senior management should see both absolute values and movement by merchant, cohort, channel and geography.

Control assurance should focus on the transaction thesis and major risks. Internal audit or independent review can test safeguarding, merchant onboarding, financial crime, revenue, data security and resilience. Findings need due dates, accountable owners and validation of closure.

Board reporting should separate operational incidents from structural trends and clearly identify management estimates. A well-designed information system allows commercial growth and control performance to be considered together.

24. Execute a 100-day value and control plan

The first 100 days should sequence stabilisation, evidence, remediation and value creation. The first month can confirm cash, settlement, access, key counterparties, merchant retention and regulatory commitments. The second month can implement agreed pricing, routing, procurement, compliance and reliability initiatives. The third phase can begin selected platform and merchant migrations after readiness tests.

Each initiative should have an owner, baseline, target, dependency, cost, risk and decision gate. Financial benefits should be measured through contribution and cash, not gross volume alone. Merchant experience and control indicators should accompany savings.

The buyer should maintain a small set of integration principles covering settlement continuity, regulatory compliance, data integrity, merchant communication and reversible change. Escalation should be rapid where a change affects funds or authorisation.

The plan should preserve optionality. A migration can pause if error or attrition thresholds are breached. A vendor renegotiation can proceed after contingency arrangements are ready. Value can be captured through disciplined sequencing rather than simultaneous change.

Table 4. Compliance and merchant-diligence issue map

Finding	Evidence required	Value or risk effect	Response
declining cohort retention	transaction, pricing and merchant-contact history	lower forecast volume and contribution	cohort reset, retention plan and earn-out definition
unverified net take rate	contracts, pass-through statements and ledger	uncertain revenue quality	independent bridge and valuation haircut
safeguarding breaks	liability files, bank statements and exception logs	cash shortfall and licence risk	top-up, remediation, condition and monitoring
concentrated platform dependency	merchant hierarchy, integration and contract	correlated churn and repricing exposure	consent, diversification and scenario adjustment
compliance backlog	alerts, cases, QA and regulator correspondence	remediation cost and operating restriction	costed plan, escrow and governance

Responses should be calibrated to verified severity, legal advice and the transaction structure.

Table 5. Illustrative 100-day plan for a GCC payments transaction

Period	Control priorities	Value priorities	Decision evidence
days 1 to 15	settlement, safeguarding, access, incidents and regulatory commitments	confirm merchant and revenue baseline	signed reconciliations, key-person coverage and merchant watchlist
days 16 to 30	close critical compliance and security gaps	protect concentrated merchants and partner relationships	remediation tests, consents and retention evidence
days 31 to 60	strengthen monitoring, resilience and vendor governance	price, routing and procurement pilots	controlled pilot results and contribution bridge
days 61 to 100	validate control sustainability and migration readiness	scale proven initiatives and selected cross-sell	independent assurance, merchant outcomes and cash evidence
beyond day 100	complete agreed architecture and data changes	platform consolidation and growth investment	board-approved business case and stage gates

Timing is indicative and should follow approvals, risk and operational readiness.

25. A decision framework for the investment committee

The investment committee should receive a connected answer to five questions. First, does the target have the legal and operational right to provide the services that create value? Second, does transaction-level evidence reconcile volume to net revenue, contribution and cash? Third, are settlement balances safeguarded and operationally available only for their permitted purpose? Fourth, are merchant cohorts, concentration and dependencies consistent with the forecast? Fifth, can identified control and integration work be funded and executed without disrupting payments?

The recommendation should distinguish verified evidence, open items and hypothetical analytical assumptions. It should show how each material finding affects valuation, structure, conditions, integration and monitoring. A red flag may be curable with cash and governance, or it may undermine the operating licence or revenue base. The conclusion should state the mechanism.

GCC payments markets are supported by growing electronic transaction activity and evolving infrastructure. That backdrop can create opportunity while target value remains specific to merchant relationships, net economics, regulatory permissions, technology and execution. A disciplined transaction process converts those elements into an auditable case.

The strongest decision package is reproducible. A reviewer should be able to move from a valuation output back to merchant cohorts, transaction records, contracts, settlement and source evidence. That chain supports negotiation, financing, closing and post-close value creation.

References

[1] Central Bank of the UAE, Retail Payment Services and Card Schemes Regulation, effective 1 August 2022, https://rulebook.centralbank.ae/en/rulebook/312-retail-payment-services-and-card-schemes-regulation

[2] Central Bank of the UAE, Payments and Settlements Regulations and Standards, https://www.centralbank.ae/en/our-operations/payments-and-settlements/regulations-and-standards/

[3] Central Bank of the UAE, Article 156, Retail and Wholesale Payment Operations and Related Digital Services, 2025, https://rulebook.centralbank.ae/en/rulebook/article-156-retail-and-wholesale-payment-operations-and-related-digital-services

[4] Central Bank of the UAE, Article 14, Obligations towards Retail Payment Service Users, https://rulebook.centralbank.ae/en/rulebook/article-14-obligations-towards-retail-payment-service-users

[5] Central Bank of the UAE, Guidance for Licensed Financial Institutions on Risks Relating to Payments, https://rulebook.centralbank.ae/en/rulebook/guidance-licensed-financial-institutions-risks-relating-payments

[6] Central Bank of the UAE, Annual Report 2025, https://centralbank.ae/media/4qbn11cl/annual-report-2025-en.pdf

[7] Central Bank of the UAE, Article 39, Amendment to the Retail Payment Services and Card Schemes Regulation and Stored Value Facilities Regulation, https://rulebook.centralbank.ae/en/rulebook/article-39-amendment-retail-payment-services-and-card-schemes-regulation-and-stored-value

[8] Saudi Central Bank, Law of Payments and Payment Services, https://rulebook.sama.gov.sa/en/law-payments-and-payment-services

[9] Saudi Central Bank, Implementing Regulations of the Payments and Payment Services Law, https://rulebook.sama.gov.sa/en/implementing-regulations-payments-and-payment-services-law

[10] Saudi General Authority for Competition, Economic Concentration Review Guidelines, https://gacbep.gac.gov.sa/cms/b9376edc-79a1-4573-a36d-4f3effaba838.pdf

[11] Saudi Central Bank, Payments regulatory and supervisory framework, https://rulebook.sama.gov.sa/en

[12] Saudi Central Bank, Electronic Payments Account for 85% of Retail Payments in 2025, https://sama.gov.sa/en-US/MediaCenter/News/Pages/news-1139.aspx

[13] Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, February 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Feburary%202025%20FATF%20Recommendations.pdf

[14] UAE Ministry of Economy and Tourism, Economic Concentration, https://www.moet.gov.ae/en/economic-concentration

[15] UAE Cabinet, Decision No. 3 of 2025 on thresholds related to Federal Decree-Law No. 36 of 2023, https://www.moet.gov.ae/documents/20121/0/Cabinet%2BDecision%2BNo.%2B%283%29%2Bof%2B2025%2BOn%2Bthe%2BThresholds%2BRelated%2Bto%2Bthe%2BImplementation%2Bof%2BFederal%2BDecree-Law%2BNo.%2B%2836%29%2Bof%2B2023%2BRegulati.pdf/0f228724-8dd5-9b9c-0ed8-0b94d5ae0873

[16] IFRS Foundation, IFRS 15 Revenue from Contracts with Customers, https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

[17] IFRS Foundation, Post-implementation Review of IFRS 15, including principal-versus-agent considerations, https://www.ifrs.org/content/dam/ifrs/project/pir-ifrs-15/rfi-iasb-2023-4-pir-ifrs-15.pdf

[18] Adyen, Annual Report 2024, https://investors.adyen.com/financials/2024

[19] Adyen, Fraud's Identity Crisis, methodology and platform data, 2026, https://www.adyen.com/press-and-media/fraud-report-2026

[20] Block, Q4 2024 Shareholder Letter and 2024 operating metrics, https://investors.block.xyz/files/doc_financials/2024/q4/Shareholder-Letter_Block-4Q24pdf.pdf

[21] PCI Security Standards Council, Payment Card Industry Data Security Standard, https://www.pcisecuritystandards.org/standards/pci-dss/

[22] EMVCo, EMV Payment Tokenisation, https://www.emvco.com/emv-technologies/payment-tokenisation/

About the Author

Authored by Chennakeshav Adya, Independent Researcher

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds, bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.