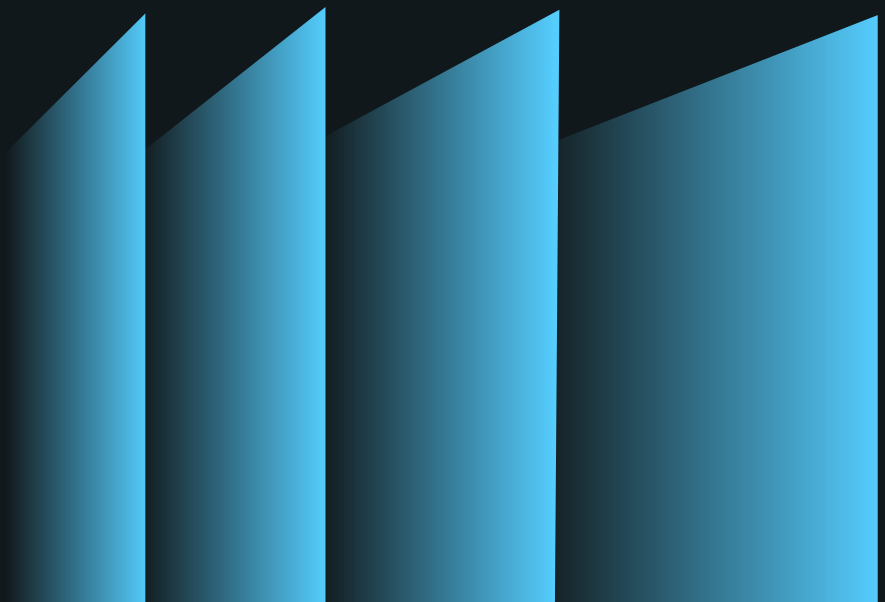
Converged on Paper

Fraud and Cybersecurity in Quick Service Restaurants



Accertify

Study Background

The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers (Accertify + Liminal, 2026) examined whether managing fraud and cybersecurity as separate disciplines is costing organizations money — and found that it is. Across 250 fraud and risk decision-makers spanning five verticals, the study identified four specific convergence behaviors that predict performance: sharing responsibility for two or more threat use cases, unifying data between fraud and cyber teams, elevating fraud risk to the Board agenda, and integrating organizational structure. The order matters: the path to peak performance runs through shared use case ownership first, followed by data integration and Board engagement together, with structural integration last. Organizations that lead with structure before those foundations are in place perform worse than those that do nothing at all. Organizations that get the sequence right — the study's Elite tier — score 3.4x higher on the Precise Yes Score, a benchmark measuring dollars approved per dollar of fraud loss, than those with no convergence behaviors in place. For full methodology, the convergence framework, and cross-vertical analysis, see the main report.

Quick Service Restaurants: Key Findings

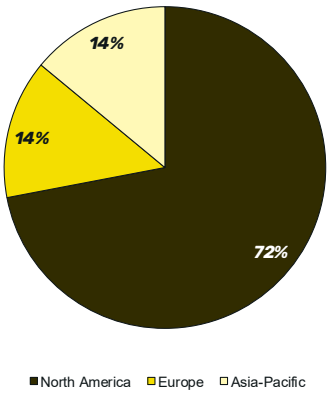
The QSR/Restaurants vertical (n=50) tells a story of an industry that looks converged on paper without yet converging where it matters. QSR leads every vertical in the study on structural integration, CISO ownership, and self-reported solution alignment - and is a close second on procurement alignment. QSR is also the most confident vertical in the study about its ability to manage fraud threats, today and looking ahead. Yet QSR also has the highest concentration of organizations stuck in Convergence "Purgatory" of any vertical (52%), and its apparently strong fraud precision collapses on inspection: QSR's median Precise Yes score is closely clustered with the three lowest-performing verticals. QSR's drive toward convergence is itself reactive rather than anticipatory: its leading drivers are budget and tool consolidation and a major incident or breach, both cited well above the rest of the study. Bot/credential stuffing is QSR's defining threat, yet is notably absent from QSR's own platform-unification priorities, which lean toward CNP fraud and promo/loyalty abuse instead.

1. Who's in the Room

The QSR Sample

The Restaurants & Food Service sample (n=50) consists entirely of Quick Service Restaurant operators. 72% of respondents are based in North America, with Asia-Pacific and Europe each accounting for 14%.

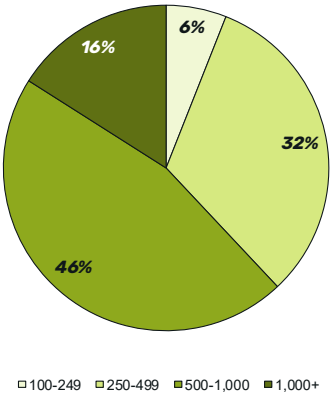
What region is currently the highest priority for your team based on revenue contribution?



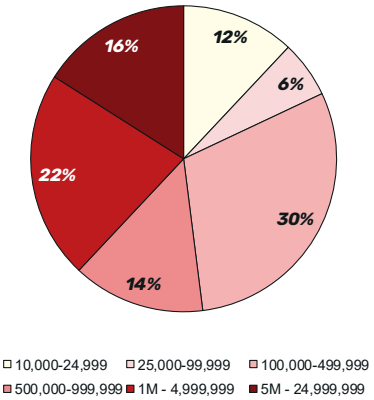
Source: The Convergence Dividend, Accertify + Liminal, 2026. QSR sample, n=50.

Organizations in this sample tend toward the mid-size range. 84% have fewer than 1,000 employees globally, with 46% concentrated in the 500–1,000 band. The customer base tells a different story: 38% of QSR respondents serve more than 1 million customers, a reflection of the high transaction volumes and broad reach that characterize quick service at scale.

Approximately how many employees does your organization have globally?



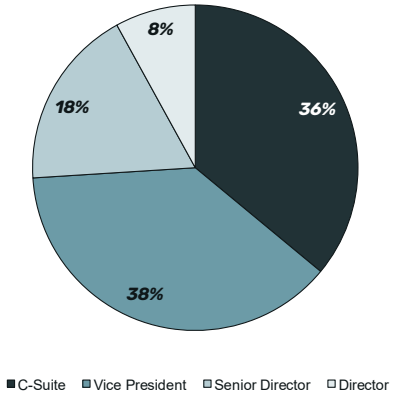
Approximately how many individual customers does your company currently have?



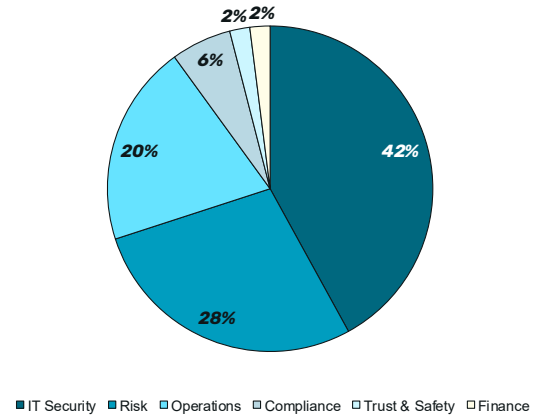
Source: The Convergence Dividend, Accertify + Liminal, 2026. QSR sample, n=50.

Respondents skew toward VP level (38%) ahead of C-Suite (36%), with Senior Directors at 18%. By function, IT Security accounts for 42% of respondents and Risk for 28%, with Operations at 20%. QSR has the highest concentration of IT Security respondents of any vertical in the study (42%), which is worth keeping in mind as a frame for the data that follows.

What level most closely aligns with your job level?



With which business unit are you most closely associated?



Source: The Convergence Dividend, Accertify + Liminal, 2026. QSR sample, n=50.

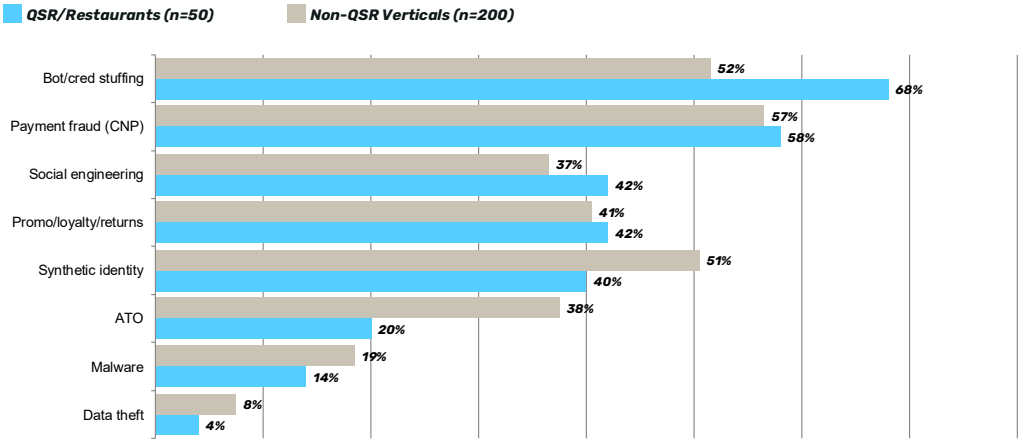
2. QSR

The Threat Landscape

Bot/credential stuffing is the defining fraud threat for QSR operators. 68% of respondents cite it as a top discussed threat, 16 points above the non-QSR verticals. Payment fraud/CNP is a close second at 58%, broadly consistent with the study overall. Account takeover, the signature threat for the Retail/e-commerce vertical, registers at just 20% in QSR, the lowest of any vertical.

Bot/Credential Stuffing Is QSR's Defining Threat

% citing each as a top discussed threat: QSR/Restaurants vs. non-QSR (n=200)

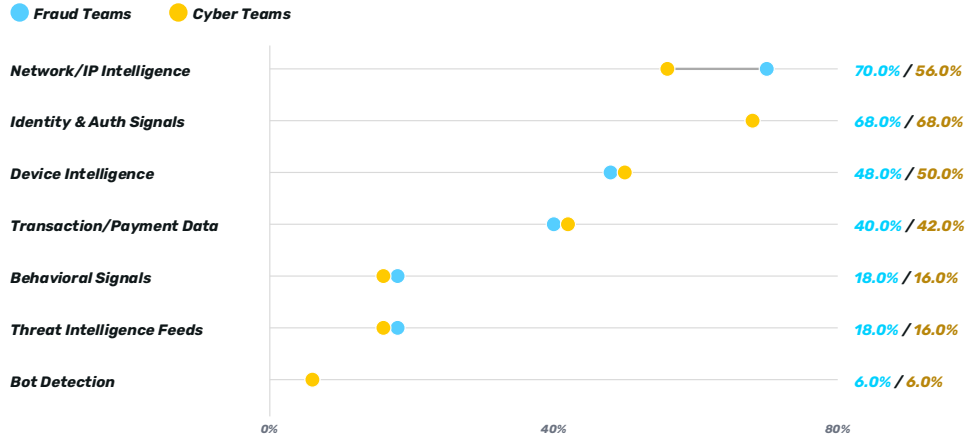


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

The signal stack QSR fraud teams rely on reflects this threat profile directly. Network/IP intelligence is the leading fraud signal at 70%, and identity and authentication signals close behind at 68% - both consistent with a threat environment built around bot/credential stuffing, which is fundamentally a login-layer attack. Behavioral signals are used by just 18% of QSR fraud teams.

QSR Fraud and Cyber Teams Converge on the Same Signals

% of QSR/Restaurant respondents citing each signal as actively used, by team - n=50

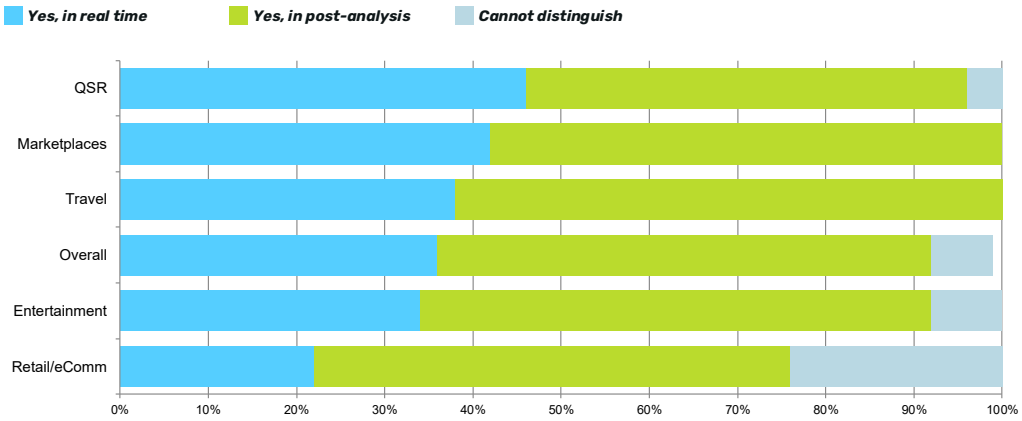


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR/Restaurants, n=50.

QSR respondents are also the most able to attribute attacks in real time. 46% say they can distinguish a fraud attack from a cyber attack as it happens - the highest rate of any vertical. Only 4% say they cannot distinguish them at all. Again, this is consistent with a threat environment dominated by automated bot attacks, which tend to be more machine-identifiable than human-driven fraud.

QSR Leads All Verticals on Real-Time Attack Attribution

Ability to distinguish fraud vs. cyber attack: all verticals, n=250



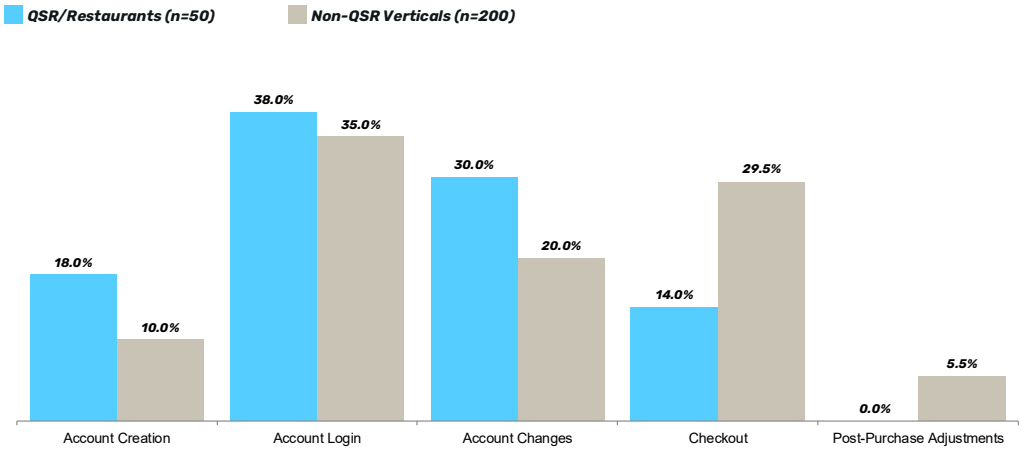
Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. n=250.

3. Where Fraud Controls Are Today in QSR… and Where They're Heading

Both QSR and non-QSR verticals identify account login as their top current priority (38% vs. 35%), but they diverge sharply on the rest: QSR puts more weight on account changes (30% vs. 20%) and far less on checkout (14% vs. 29.5%) than the rest of the study.

QSR Controls Concentrate at Login and Account Changes Today

% identifying each stage as primary point of control today: QSR vs. non-QSR (n=200)

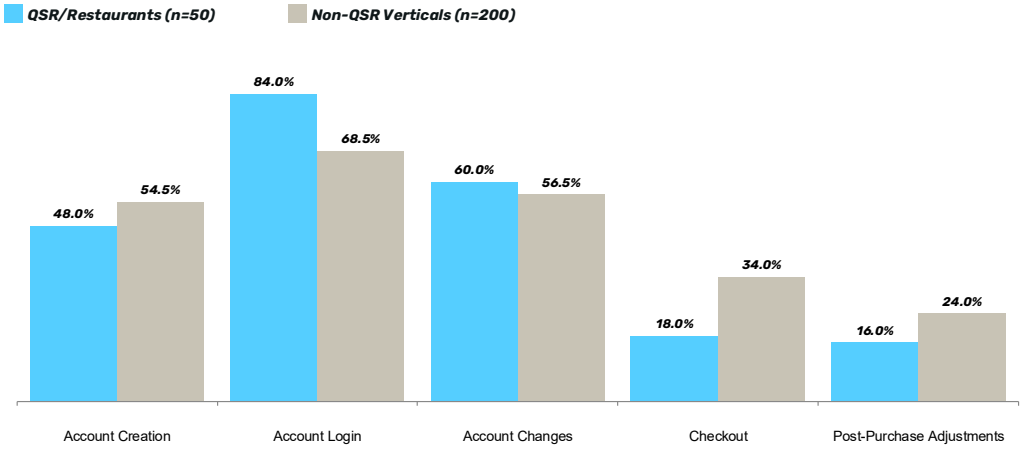


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

Expansion plans sharpen this focus rather than redirecting it. 84% of QSR respondents are expanding controls into account login - the highest expansion rate for any single stage in the study - followed by account changes (60%) and account creation (48%). Checkout and post-purchase adjustments remain QSR's lowest expansion priorities, at 18% and 16% respectively, compared to 34% and 24% for non-QSR verticals. QSR is investing further into the front end of the customer journey, where its signature threat of bot/credential stuffing originates, rather than following the checkout-centric pattern seen elsewhere in the study.

QSR Is Doubling Down on the Front End of the Journey

% expanding controls into each stage: QSR vs. non-QSR (n=200)

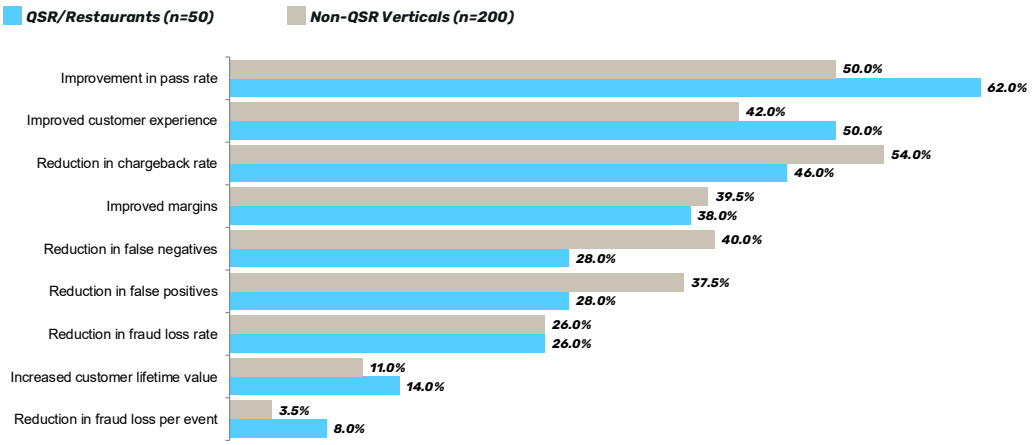


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

When evaluating fraud and cybersecurity investment more broadly, improvement in pass/approval rate is QSR's top-cited ROI outcome (62%, vs. 50% non-QSR), followed by improved customer experience (50% vs. 42%).

QSR Evaluates Fraud and Cyber Investment on Pass Rate

% citing each as a critical ROI outcome when evaluating fraud and cyber investments: QSR vs. non-QSR (n=200)

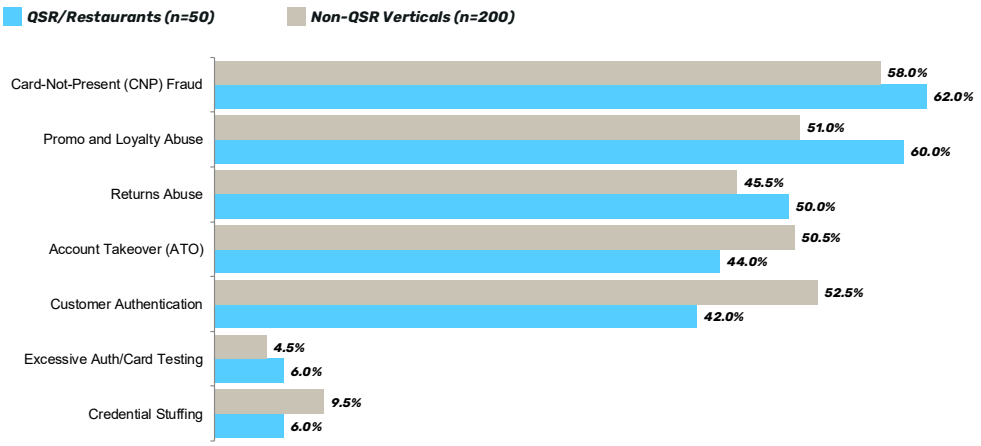


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

QSR's appetite for a unified platform is highest for CNP fraud (62%) and promo/loyalty abuse (60%), with account takeover and customer authentication close behind (44% and 42%). The notable exception is bot/credential stuffing - the threat QSR cites more than any other vertical in the study, and the use case with the weakest shared fraud-cyber ownership found earlier in this section - which ranks last among QSR's platform priorities at just 6%, below even the non-QSR rate (9.5%). It is a surprising gap: the threat QSR identifies as its own defining problem is the one least represented in what QSR wants a unified platform to solve.

QSR's Signature Threat Is Missing From Its Own Platform Priorities

% saying a unified platform for each use case would deliver an advantage: QSR vs. non-QSR (n=200)



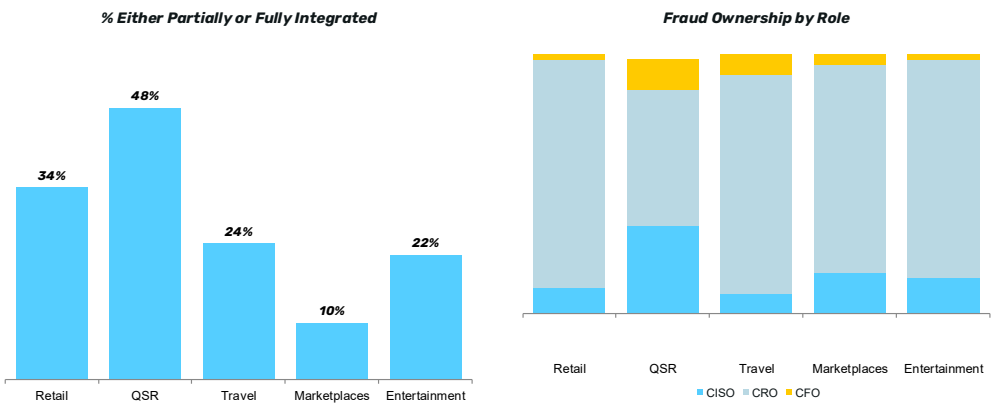
Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

4. Ownership, Structure, and Alignment

QSR has the most structurally integrated fraud and cybersecurity functions in the study: 48% of QSR organizations report partially or fully integrated structure, the highest of any vertical, well ahead of Retail (34%), Travel (24%), Entertainment (22%), and Marketplaces (10%). That structural integration is matched by ownership: fraud sits with a CISO in 34% of QSR organizations - also the highest of any vertical - and with a CRO in just 52%, the only vertical where CRO ownership dips below 80%.

QSR is Most Structurally Integrated and Fraud is Owned by the CISO More Often Than in Other Verticals

Structural integration and fraud ownership by vertical, n=50 each

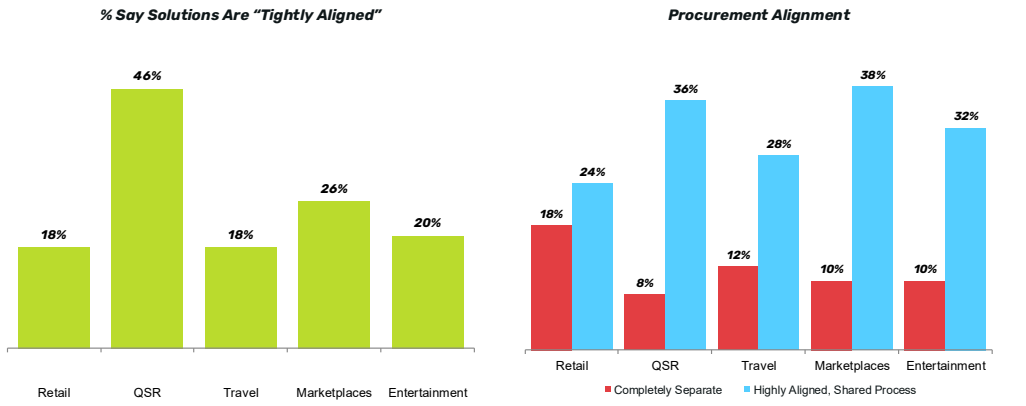


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. n=50 per vertical.

This shows up directly in how QSR respondents describe their own tools: 46% call their fraud and cybersecurity solutions tightly aligned, more than 15 points ahead of the next-highest vertical (Marketplaces, 26%) and more than double Retail (18%) or Travel (18%). Procurement reflects the same pattern rather than contradicting it: QSR has the lowest rate of "completely separate" procurement of any vertical (8%) and the second-highest rate of a fully shared evaluation and approval process (36%, behind only Marketplaces at 38%). Structure, ownership, self-perceived alignment, and procurement all point the same direction for QSR.

QSR's Structure Shows Up in How Aligned It Feels

Self-reported solution alignment and procurement alignment by vertical, n=50 each

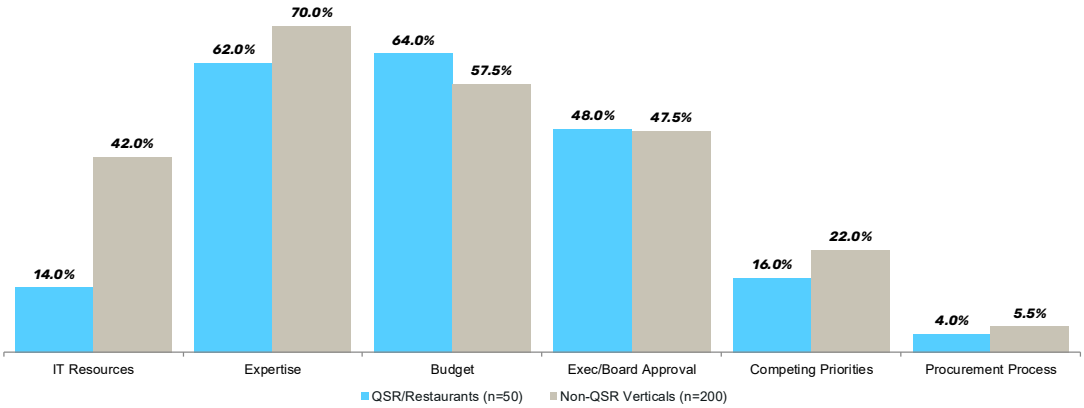


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. n=50 per vertical.

Resource constraints around fraud prevention solutions reveal a distinct pattern for QSR. It reports the lowest IT-resource constraint of any vertical (14% vs. 42% non-QSR), but a higher budget constraint than the rest of the study (64% vs. 57.5% non-QSR). QSR is not short on implementation capacity for fraud tools; it lacks funding, and, to a lesser extent, expertise (62%, slightly below the 70% non-QSR rate). Combined with QSR's high structural integration across fraud and cyber functions, this is consistent with lean-budget consolidation: a single executive absorbing both functions because QSR cannot afford to staff and fund them separately.

QSR's Constraint Is Budget, Not IT Capacity

% citing each as a significant resource constraint when considering fraud prevention solutions: QSR vs. non-QSR (n=200)



Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

5. QSR Performance

Across the five verticals in this study, the metrics fraud teams track every day appear almost negligible in their differences. Approval rates range from 97.5% to 98.2%. Fraud chargeback rates range from 15.9 to 24.9 basis points. Legitimate customer pass-through rates cluster between 90.8% and 94.2%. Manual review rates sit between 1.69% and 2.49%. On the surface, these are five industries performing in roughly the same range.

How Industries Differ in Fraud Performance

Fraud Metric	Retail / eCommerce	Entertainment & Media	Marketplaces	Travel	Restaurants / Food Service
Dollar Volume Approval Rate	98.2%	97.5%	97.8%	97.7%	97.8%
Fraud Chargeback Rate (Dollars)	15.9 bps (.159%)	23.7 bps (.237%)	24.9 bps (.249%)	23.2 bps (.232%)	23.4 bps (.234%)
Legitimate Customer Pass-Through Rate	94.2%	94.2%	90.8%	93.3%	94.2%
Manual Review Rate	1.90%	2.00%	1.87%	1.69%	2.49%

Source: The Convergence Dividend, Accertify + Liminal, April 2026. N=250

They are not. The problem with evaluating fraud performance on these metrics in isolation is that approval rate and fraud chargeback rate move in opposite directions — a team that declines more transactions will lower its fraud rate but also suppress its approval rate, and vice versa. What matters is how well an organization holds both simultaneously. A vertical with a 98.2% approval rate and a 15.9 bps fraud chargeback rate is doing something fundamentally different from one with a 97.5% approval rate and a 23.7 bps rate — but that gap is invisible if you look at either metric alone.

The Precise Yes Score (or PYS) was constructed to surface exactly that difference. Calculated as approval rate divided by fraud chargeback rate - both expressed as percentages of total dollars transacted - it produces a single number representing dollars approved per dollar lost to fraud chargeback. Higher is better. It rewards organizations that say yes more precisely, not just more often.

The "Precise Yes" Score

Approved Dollar Volume %
What % of transaction dollars did you approve?

÷

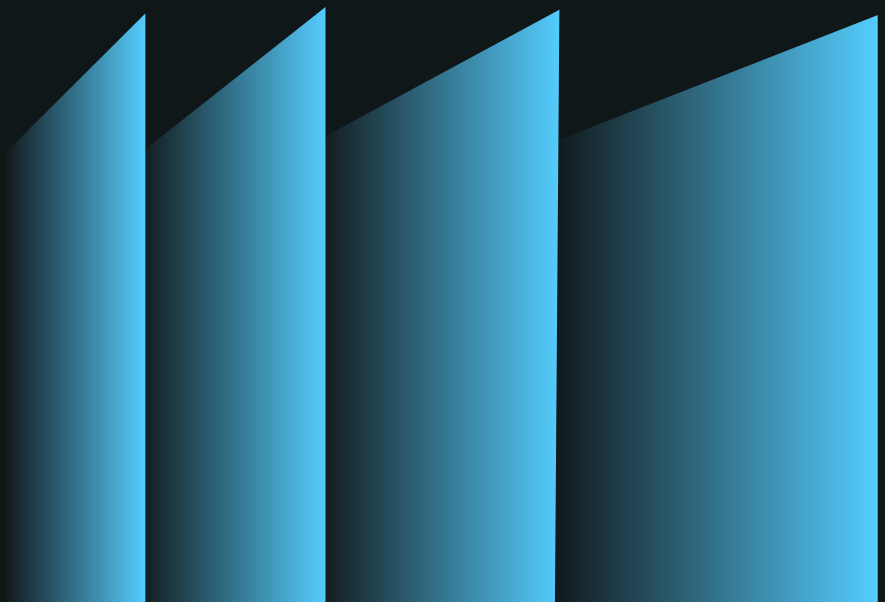
Fraud Chargeback Rate %
What % of transaction dollars were lost to fraud?

=

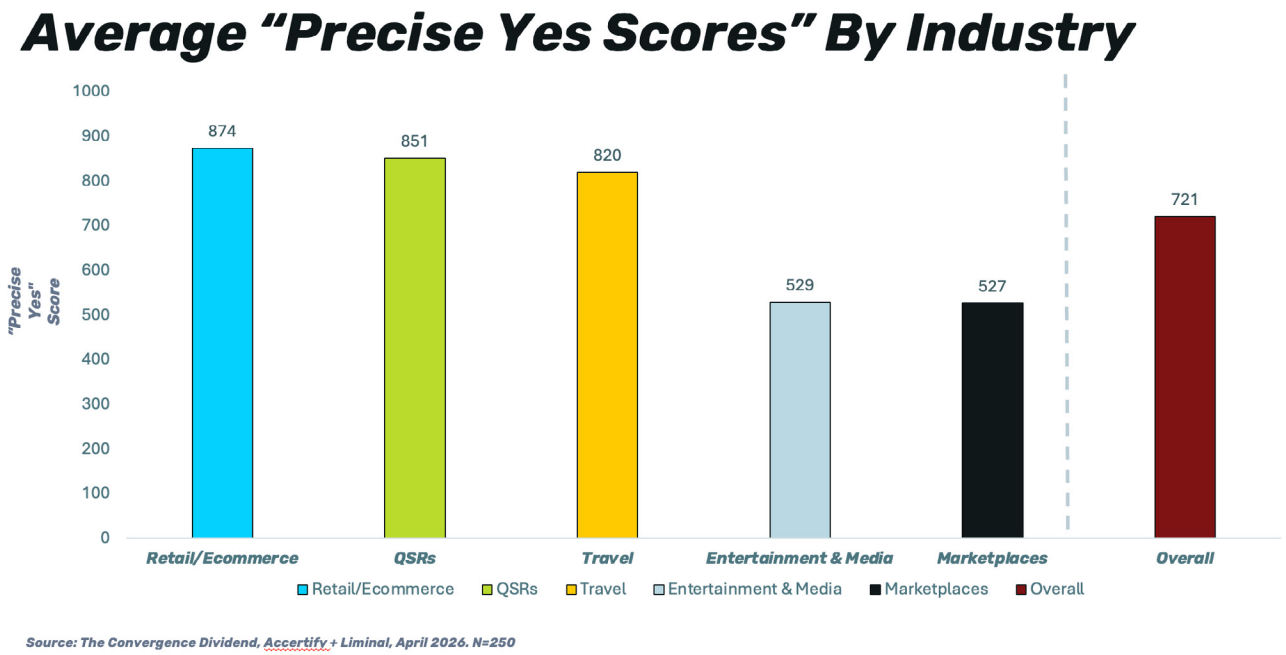
"Precise Yes" Score
Approved dollars per dollar of fraud loss

Higher score = more precise, confident, data-backed yes.

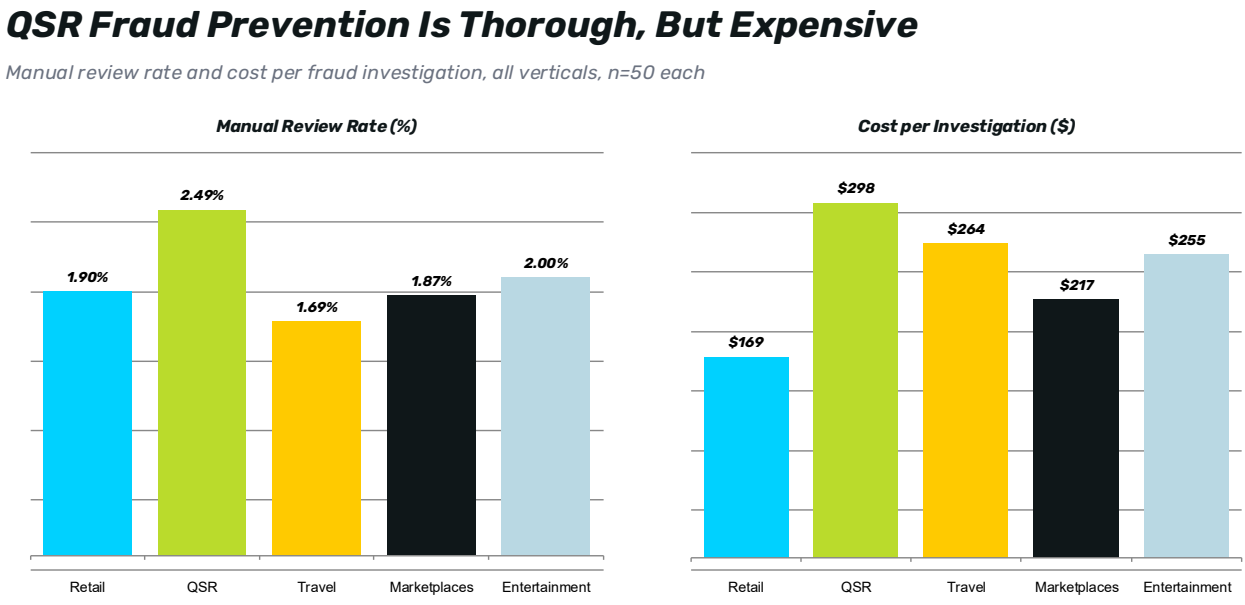
Precision, Not Just Protection



On that measure, Retail/eCommerce stands apart. With a mean PYS of 874, Retail approves $874 for every dollar lost to fraud chargeback — the highest of any vertical in the study, and 66% higher than Marketplaces at 527 and Entertainment at 529.

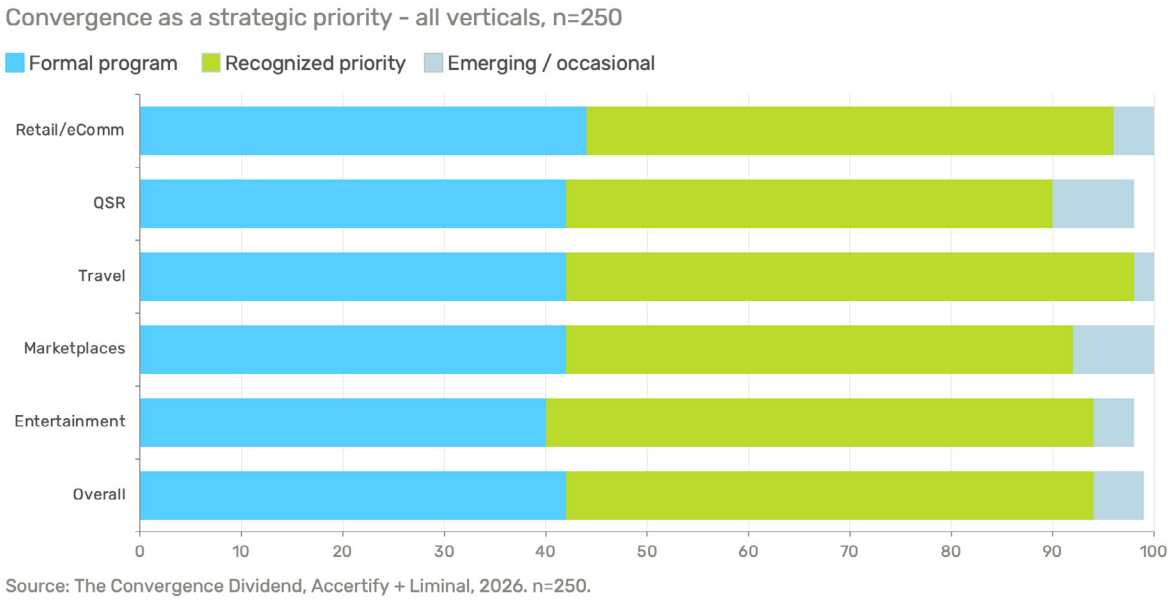


QSR is also the most expensive vertical to operate per fraud case: cost per investigation runs $298, the highest of any vertical, well above Retail ($169) and Travel ($264). Yet this expense does not translate into friction for legitimate customers: QSR ties Retail and Entertainment for the highest legitimate customer pass-through rate in the study (94.2%), despite reviewing more transactions manually than any other vertical (2.49% manual review rate, also the highest). QSR runs a more expensive, more manual review process than its peers without turning away more good customers than the rest of the study.



6. The Drive Toward Fraud-Cyber Convergence

QSR's convergence program status roughly matches the rest of the study: 42% report a formal program, identical to the non-QSR rate, while 48% call it a recognized priority (vs. 53% non-QSR) and 8% call it emerging or occasional (vs. 4.5% non-QSR). QSR is neither ahead of nor behind the field on placing strategic priority on convergence.

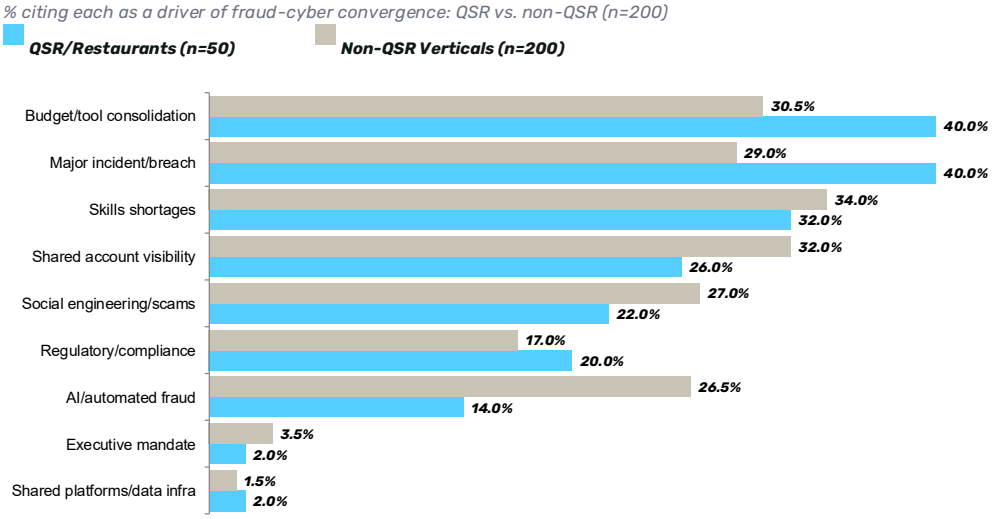


Source: The Convergence Dividend, Accertify + Liminal, 2026. n=250.

What's driving that convergence differs sharply from the rest of the study, though. QSR's two leading drivers are budget/tool consolidation (40%) and a major incident or breach (40%), both well above the non-QSR rates of 30.5% and 29.0% respectively. This is a reactive profile: QSR organizations are converging in response to cost pressure or to something that already happened. Notably, AI/automated fraud registers as QSR's lowest-ranked driver (14%, vs. 26.5% non-QSR), despite QSR's threat landscape being dominated by bot/credential stuffing (Section 2). Interestingly, the vertical facing the most automated threat is also the least likely to cite automation as a reason to converge.

Reactivity: Budget Pressures and Major Fraud/Cyber Incidents Are Main Drivers of Fraud-Cyber Convergence in QSR

% citing each as a driver of fraud-cyber convergence: QSR vs. non-QSR (n=200)

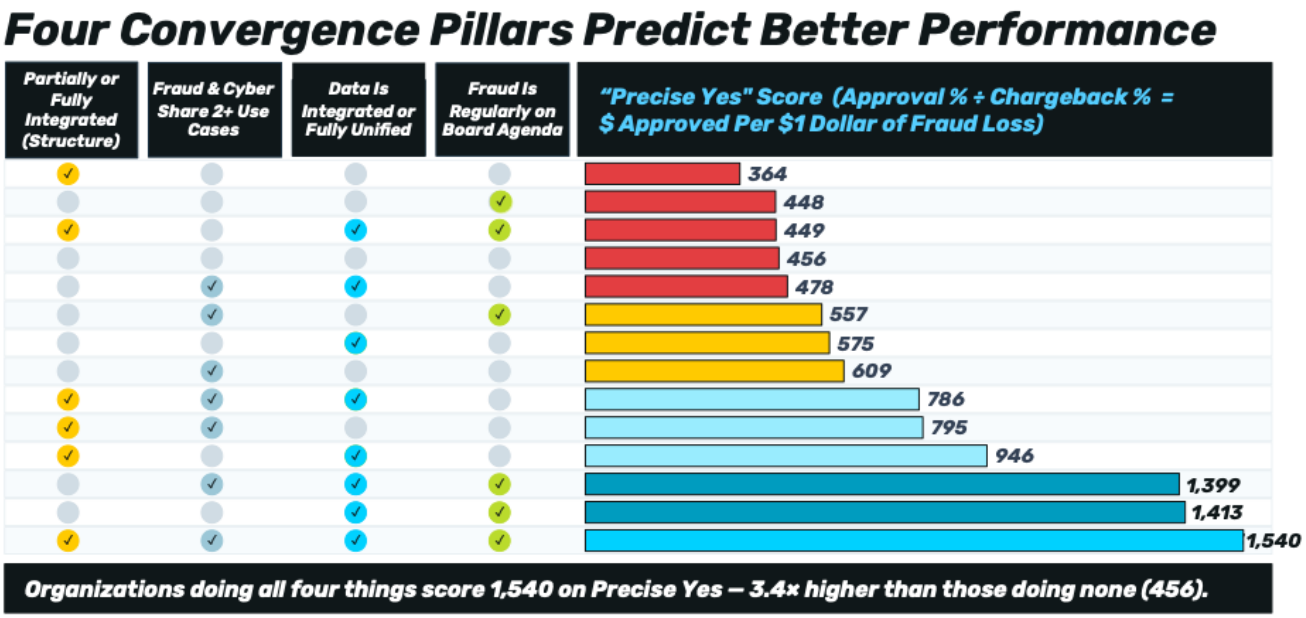


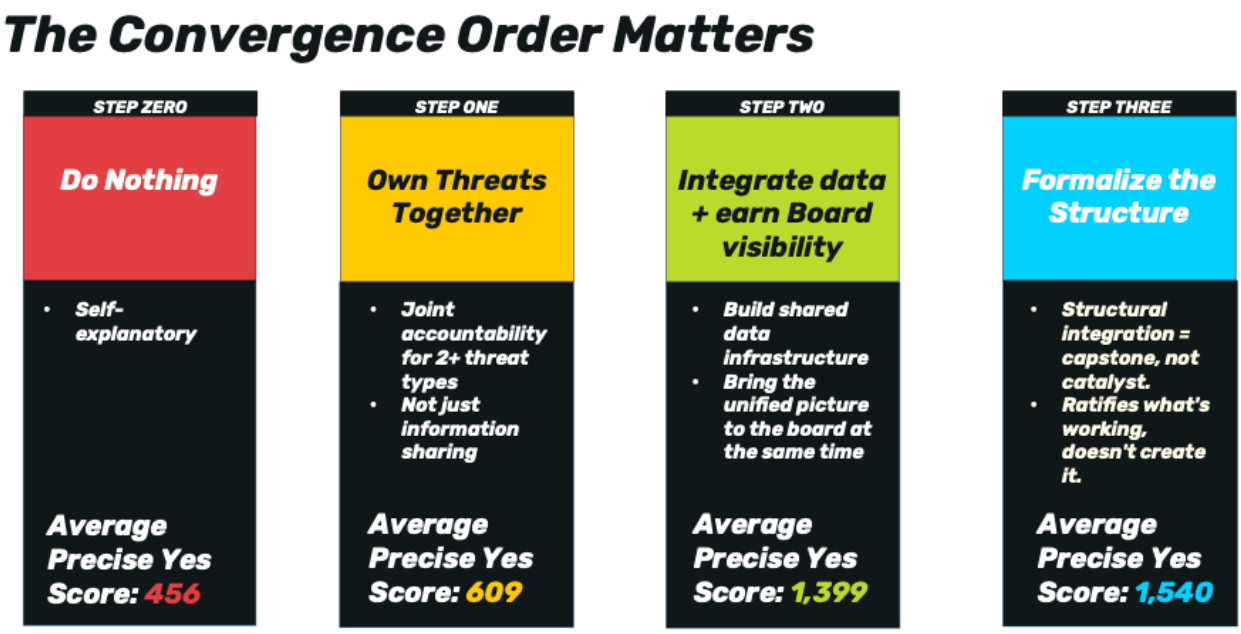
Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

7. How Converged QSR Actually Is

The Four Pillars

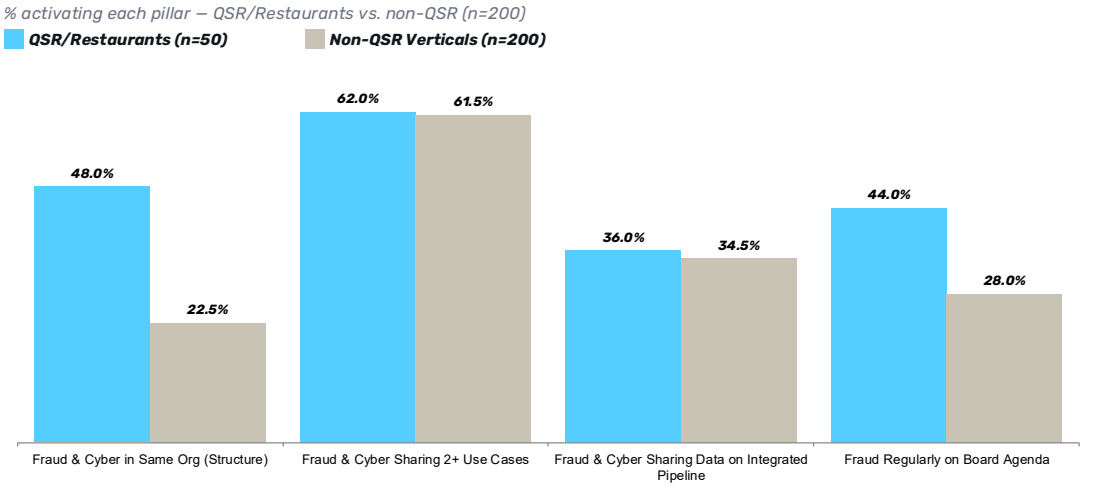
The main fraud-cyber convergence study identified four specific organizational behaviors associated with meaningfully better fraud performance, and showed that the combination and sequence in which organizations adopt them matters as much as whether they adopt them at all. The chart below shows how the Precise Yes Score changes across every combination of these four pillars. The pattern is unambiguous: organizations with all four activated place score 3.4× higher than those with none, and the right sequence - use cases first, data and Board together, structure last - is what separates the highest performers from those stuck in the middle.





QSR leads decisively on two of the four convergence pillars and sits at parity on the other two. 48% of QSR organizations report partially or fully integrated structure, more than double the non-QSR rate (22.5%). Board engagement is also elevated: 44% of QSR organizations discuss fraud regularly at the Board level, versus 28% non-QSR. Use-case sharing (62% vs. 61.5%) and data integration (36% vs. 34.5%) are essentially even with the non-QSR verticals.

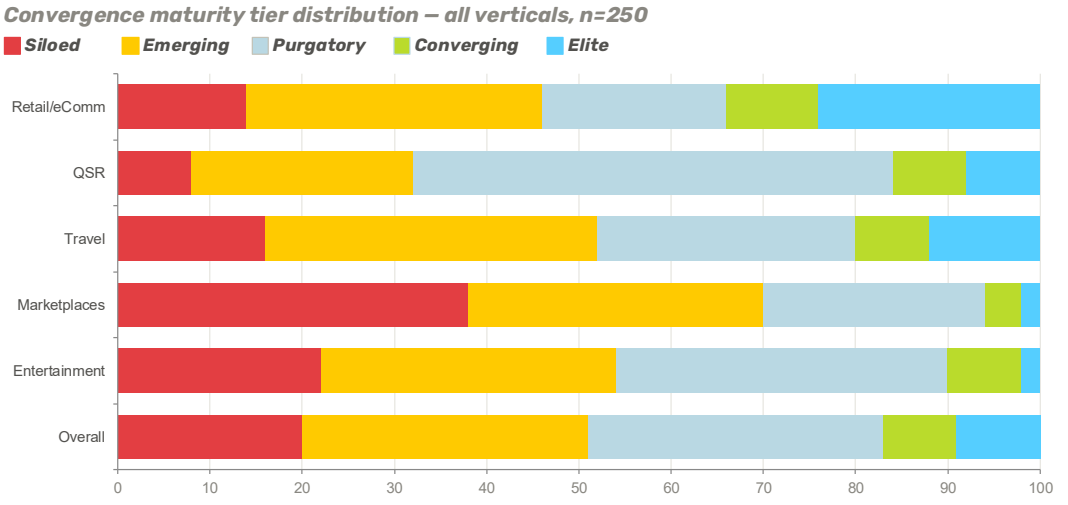
QSR Leads on Structural Convergence and Elevating Fraud to Board Agenda, In-Line on The Rest



Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

QSR has the highest concentration of organizations in "Purgatory" of any vertical: 52%, compared to 32% study-wide, and more than double Retail's "Purgatory" rate (20%). This is despite QSR also having one of the lowest Siloed rates in the study at 8%, well below the 20% study average and far below Marketplaces (38%). QSR organizations are rarely doing nothing, but only 16% combined have reached Converging (8%) or Elite (8%), both close to the study-wide averages. QSR's convergence maturity is not concentrated at the bottom; it is concentrated in the middle, doing some of the right things without doing enough of the right things together.

QSRs Have the Highest Concentration of "Purgatory" Organizations

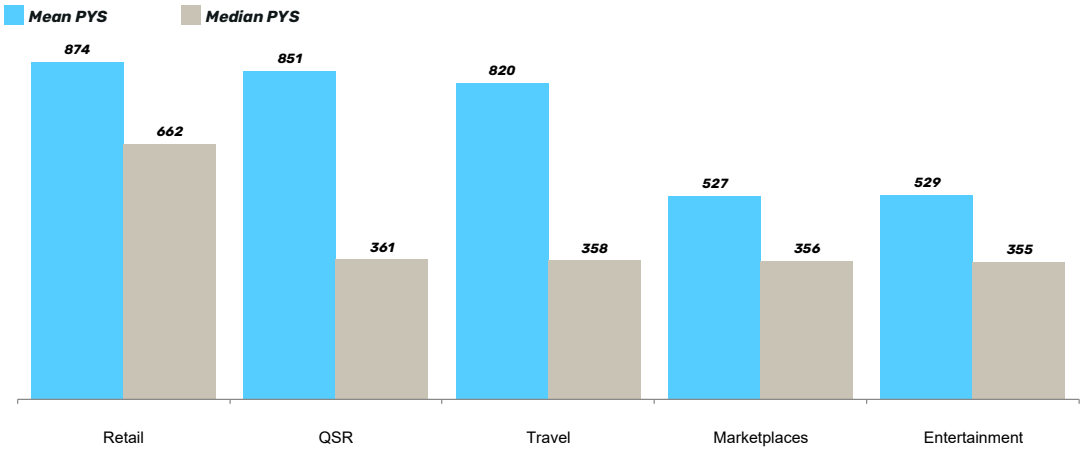


Source: The Convergence Dividend, Accertify + Liminal, 2026. n=250.

This raises an apparent tension with QSR's Precise Yes Score, where its mean (851) is the second-highest of any vertical, trailing only Retail. That mean is misleading. QSR's median PYS is 361, essentially tied with Travel (358), Marketplaces (356), and Entertainment (355), and far below Retail's median of 662, the only vertical with a robust, outlier-resistant advantage. The gap between QSR's mean and median (490 points) is the largest in the study, driven by a handful of individual respondents reporting extreme approval-to-fraud ratios scattered across every maturity tier, not by QSR's Elite or Converging organizations systematically outperforming their counterparts elsewhere. Once that distortion is removed, QSR's typical performance is consistent with its Purgatory-heavy maturity profile: unremarkable, not exceptional.

Mean Precise Yes Score Overstates QSR Performance Medians Tell a Different Story

Mean vs. median Precise Yes Score, all verticals, n=50 each

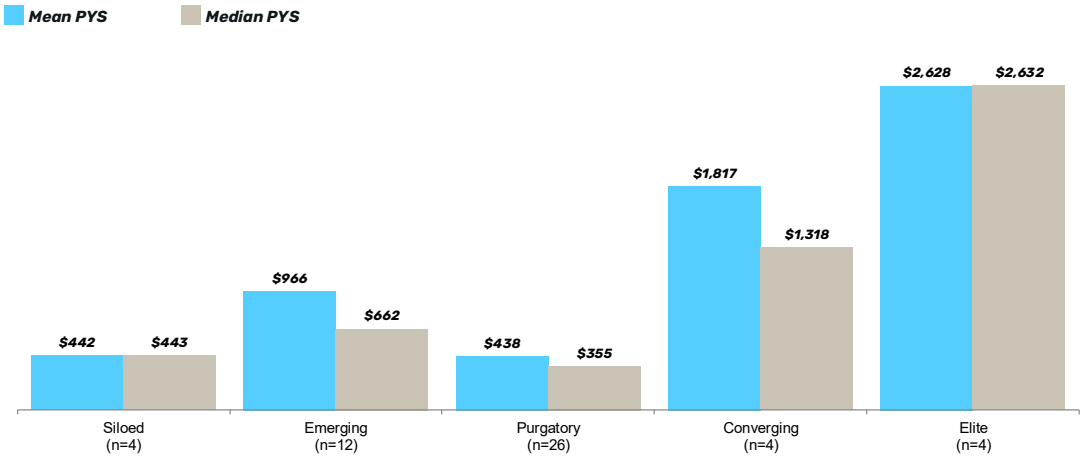


Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. n=50 per vertical.

In the end, QSR's tier-level performance data reinforces the Convergence Maturity framework. Within QSR, Siloed organizations (n=4) report a mean PYS of 442, and Purgatory organizations (n=26) report 438, rendering the two indistinguishable. The QSR vertical proves that doing some of the right things in the wrong combination delivers no advantage over doing nothing at all, an even starker version of the master framework's warning that partial or badly-sequenced convergence can be worse than staying siloed.

QSR Confirms the Convergence Maturity Framework: "Purgatory" Buys Nothing

Mean and median Precise Yes Score by convergence tier: QSR/Restaurants, n=50



Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR/Restaurants, n=50.

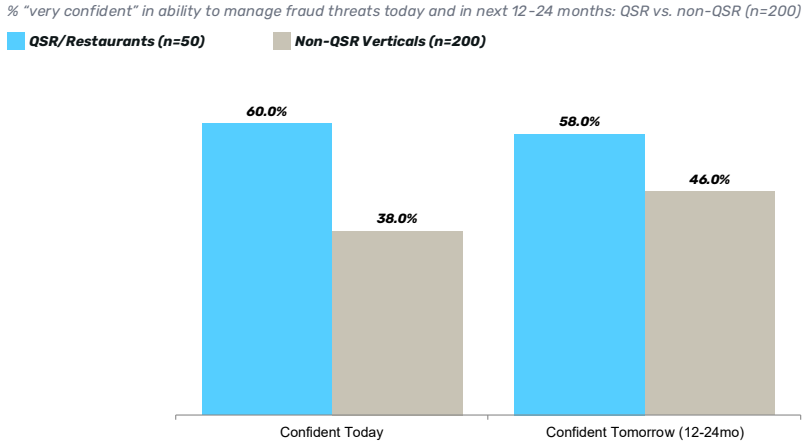
8. Looking Forward

Confidence, AI, and Agentic Commerce in QSR

QSR presents a markedly more confident profile on AI and agentic commerce than the rest of the study. 60% of QSR respondents are very confident in their organization's ability to manage fraud threats today, well above the 38% non-QSR rate. That confidence extends to the 12-24 month outlook: 58% are very confident in their preparedness for emerging threats, versus 46% non-QSR.

QSR Is the Most Confident Vertical in the Study

% "very confident" in ability to manage fraud threats today and in next 12-24 months: QSR vs. non-QSR (n=200)



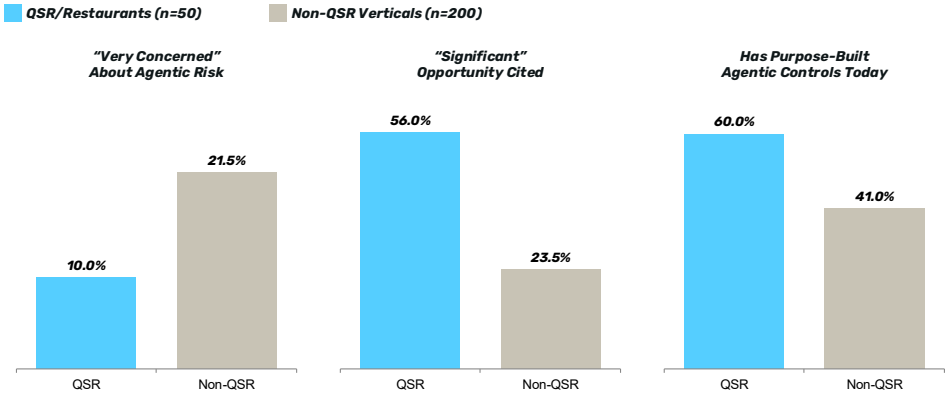
Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

This confidence pairs with lower concern and higher optimism about agentic commerce specifically. Only 10% of QSR respondents are very concerned about AI-agent fraud risk, less than half the non-QSR rate of 21.5% - the lowest concern level of any vertical in the study. At the same time, QSR sees dramatically more significant (not just moderate) opportunity from agentic commerce: 56% cite significant opportunity, more than double the non-QSR rate of 23.5%, and the highest rate of any vertical.

QSR's confidence appears to be backed by action, not just sentiment. Every QSR organization reports either purpose-built (60%) or adapted (40%) fraud controls for agentic commerce - literally NONE report having no plans - compared to 95.5% of non-QSR organizations, of which only 41% have purpose-built controls specifically.

QSR Is Least Worried and Most Prepared for Agentic Commerce

Agentic-commerce concern, opportunity, and controls: QSR vs. non-QSR (n=200)



Source: The Convergence Dividend: Quantifying What Fraud-Cyber Convergence Actually Delivers, Accertify + Liminal, 2026. QSR n=50, non-QSR n=200.

Conclusion

QSR enters the fraud-cyber convergence conversation with more of the visible signals of maturity than almost any other vertical: the highest concentration of structurally integrated organizations in the study, the highest rate of CISO ownership, and near-universal confidence that its teams can handle both today's threats and whatever comes next. That confidence is not empty: QSR is also the fastest vertical at telling a fraud attack from a cyber one in real time, and it has already built purpose-built agentic-commerce controls at a higher rate than any other vertical measured.

Yet the study's own Convergence Maturity Framework shows why QSR's visible strength hasn't yet turned into elite performance. QSR has the highest concentration of organizations stuck in Convergence "Purgatory" of any vertical, and its seemingly strong average performance score turns out to be propped up by a handful of outliers. When medians are examined, the typical QSR organization is indistinguishable from the lowest-scoring verticals in the study. Much of this may trace back to how QSR arrived at convergence in the first place: driven reactively by budget pressure and incident response. The budget pressures may have also spurred QSR to put fraud and cyber under the same organizational umbrella - and more often under the CISO.

None of this is lost ground. QSR has already cleared the step most organizations treat as the finish line - organizational structure - and its own investment priorities show real appetite for further platform investment. The opportunity ahead is to direct that same energy toward the foundation the optimal convergence sequence calls for: shared ownership of threat use cases and integrated data between fraud and cyber teams, starting with bot/credential stuffing, the threat QSR itself identifies as defining. QSR has already built the capstone. What's ahead for QSR is going back to lay the foundation beneath.

Accertify enables commerce by doing one thing extraordinarily well: pinpointing fraud. The company's Predictive Yes Platform helps businesses say yes to more - more good customers, more revenue, and more growth - without getting burned. It's a precise, confident, data-backed yes, made possible by joining signals across the entire customer lifecycle through unmatched data volume, layered AI-powered models, and a consortium approach that protects clients from bad actors spotted anywhere in the network while unlocking business with good actors verified anywhere in the network. With more than 10 billion transactions and over $1 trillion in commerce processed in 2025 alone, Accertify delivers the intelligence and precision that fraud and payments teams need to say yes confidently and enable growth. That's the More Yes difference. Learn more at **accertify.com**.

Accertify