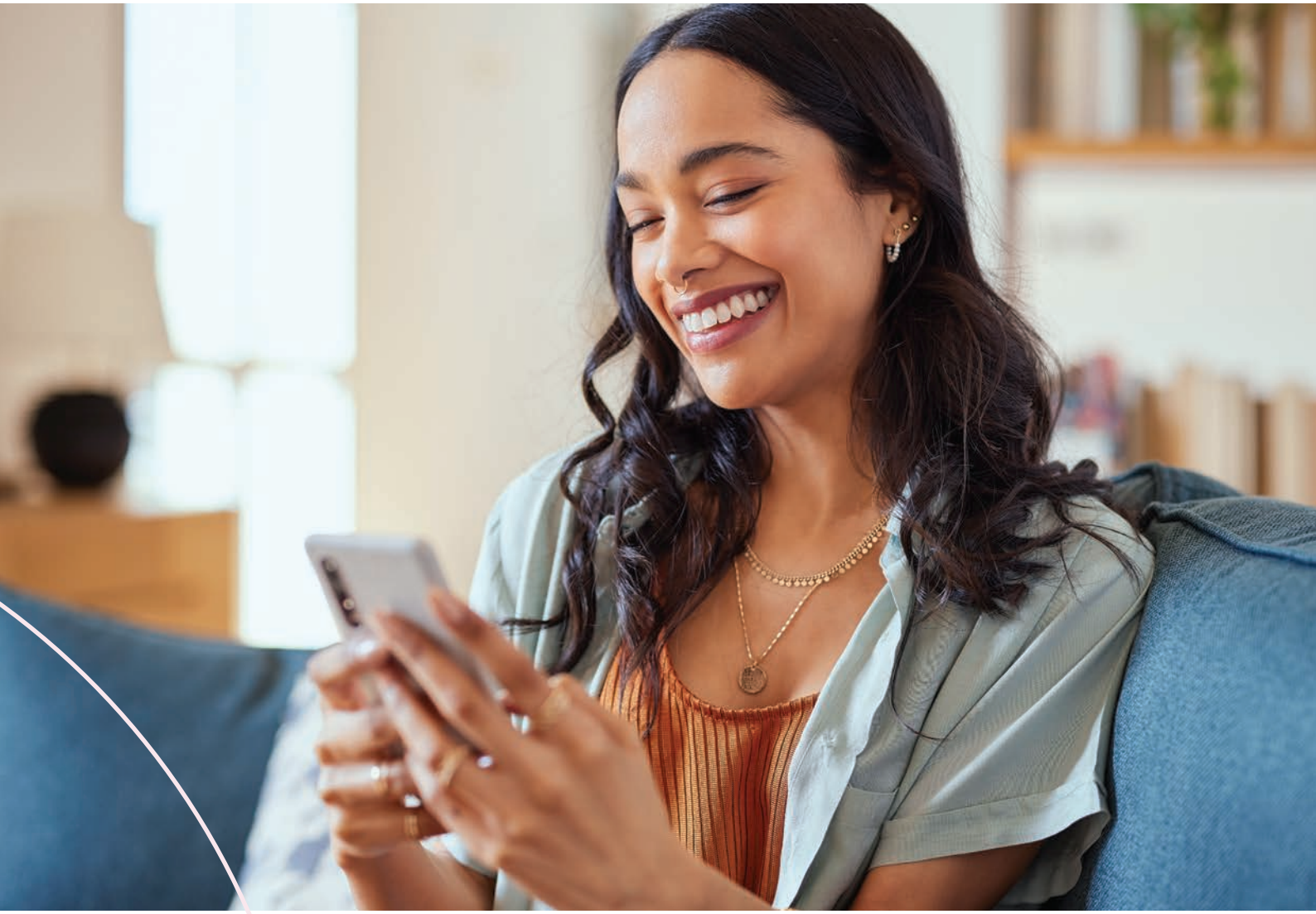
Eckoh

Beyond compliance:
Transforming payment security into competitive advantage



Building on our biennial research, last conducted in 2023, this report examines how consumer attitudes toward payment security are evolving, with particular focus on AI adoption, customer experience and the changing regulatory landscape.

Executive summary

The payment security landscape has transformed since our last study in 2023. Three converging forces are reshaping consumer expectations and organizational requirements: namely the implementation of PCI DSS 4.0.1; accelerating fraud levels that have heightened consumer security consciousness; and the rapid adoption of AI in contact centers.

Our 2025 research, comprising a survey of 401 consumers alongside comprehensive market analysis, reveals that payment security has evolved from a compliance requirement to a critical customer experience differentiator.

Key findings

Consumer security concerns remain acute

- 82% report growing concern about payment card fraud (unchanged since 2023)
- 77% prefer not to provide card details verbally to contact center agents
- 75% are reluctant to pay over the phone due to fraud risk
- Only 1 in 8 people consider reading card details to an agent "extremely secure"

77%
prefer not to provide card details verbally to contact center agents

Consumers strongly prefer technology solutions over process controls

- Consumers identify secure technology that hides card details from agents as their most preferred fraud prevention method
- 69% prefer technological security approaches over process-based methods
- Digital payment methods average 72% security confidence amongst consumers vs. 45% for agent-mediated methods

69%
prefer technological security approaches over process-based methods

AI adoption shows positive trajectory

- 42% believe AI agents can be more secure than human agents for payment processing
- 60% like resolving issues without speaking to anyone for routine transactions
- Younger consumers (under 45) show 50% security confidence in AI vs. 29% for those over 45

42%
believe AI agents can be more secure than human agents for payment processing

Persistent market challenges

Despite heightened security awareness and available technology alternatives, 25% of consumers were still asked to read card details directly to agents during their most recent phone purchase, an increase from 2023 levels. This persistence of insecure practices occurs against a backdrop of escalating threats: 269 million stolen card records were exposed in 2024, with card-not-present fraud now accounting for 65% of all credit card losses.

Simultaneously, PCI DSS 4.0.1 compliance requirements became mandatory in March 2024, expanding from 370 to over 500 requirements and significantly increasing both complexity and costs for organizations maintaining payment data in their environments.

269 million

269 million stolen card records were exposed in 2024

Strategic implications

The convergence of persistent consumer security concerns, regulatory complexity, and advancing AI capabilities creates a compelling business case for payment security solutions such as those offered by Eckoh that ensure card data never enters contact center environments and is never shared with an agent. Organizations that embrace this transformation can simultaneously address consumer preferences, eliminate compliance burden, and position themselves for the AI-enhanced customer experiences that younger demographics increasingly expect.

Rather than viewing payment security as a compliance cost, forward-thinking organizations can transform it into a competitive advantage that enhances customer trust and service delivery whilst reducing operational overhead.

The evolving threat landscape

65%
Card-not-present (CNP) fraud accounts for 65% of all credit card fraud losses

Escalating fraud levels drive consumer anxiety

The payment fraud has continued to rise since 2023. 269 million stolen card records were posted across dark and clear web platforms in 2024 (Recorded Future, 2024) and 62 million Americans experienced credit card fraud, with unauthorized purchases exceeding $6.2 billion annually (Security.org, 2025). This fraud escalation is reflected in consumer attitudes. Our survey reveals that 82% of consumers report increasing concern about payment card fraud, a statistic that remains virtually unchanged since 2023.

Contact centers as fraud vectors

Telephone and contact center transactions face particular vulnerability. Card-not-present (CNP) fraud accounts for 65% of all credit card fraud losses (Merchant Cost Consulting, 2025) and 92% of all unauthorized transactions now involve cards that weren't physically lost or stolen (Security.org, 2025). This trend directly impacts contact center operations, where traditional payment processing methods expose both organizations and consumers to fraud risk. This risk has been heightened by the much higher levels of work at home agents that were used during the pandemic and which have continued since.

Our survey data confirms consumer awareness of these vulnerabilities. When asked about fraud prevention preferences, respondents demonstrated clear understanding of contact center risks when no technology solution is in place:

- 65% report that fraud risk has on occasion stopped them from making payments over the phone
- 70% report that they are reluctant to make unsecured payments by telephone

Despite this, in 2025 a quarter of our respondents reported being asked to read card details to contact center agents during their last phone purchase, increased from 23% in 2023. This shows that, despite growing security awareness and widely available technological solutions, many organizations continue to rely on fundamentally insecure payment methods.

70%
70% report that they are reluctant to make unsecured payments by telephone

Regulatory evolution: PCI DSS 4.0.1 and compliance implications

Enhanced requirements create compliance complexity

The Payment Card Industry Data Security Standard version 4.0.1 came into force on 31 March 2024. The updated standard introduces a number of substantial changes that directly impact contact center operations *(PCI Security Standards Council, 2023)*.

Contact centers are now required to meet enhanced documentation mandates, including detailed annual confirmation of cardholder data environment scope and comprehensive role definitions for compliance responsibilities. Organizations must apply rigorous change control processes to network infrastructure and meet strengthened security standards for any third-party service providers that may access or process payment data.

Additional requirements that became mandatory in March 2025 have further intensified these compliance challenges. Contact centers must now implement expanded multi-factor authentication across all cardholder data environments and meet more stringent encryption standards that eliminate previously acceptable disk or partition-level encryption methods. Organizations are also required to establish comprehensive asset lifecycle management protocols and conduct authenticated vulnerability scanning, creating substantial operational overhead and technical complexity.

These comprehensive PCI DSS 4.0.1 requirements underscore the growing regulatory pressure on contact centers to either invest heavily in compliance infrastructure or consider de-scoping strategies that remove payment card data from their environments entirely.

This remains in line with advice from the PCI Security Standards Council which advises that

"Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves...In general no payment card data should ever be stored by the merchant unless it's necessary to meet the needs of the business" *(PCI Security Standards Council)*

This makes solutions that eliminate agent exposure to cardholder data altogether, such as Eckoh's suite of products, increasingly attractive from both security and compliance perspectives.

The compliance cost challenge

Achieving and demonstrating PCI DSS 4.0.1 compliance places significant cost and time burdens on organizations, bringing total requirements from 370 to over 500 *(Fastly, 2024)*. Maintaining compliance is expensive. An assessment from a PCI certified QSA costs on average $15,000 but enterprises can be looking at total costs of more than $250,000 for a full PCI audit and testing, plus potentially hundreds of thousands more for the remediation required to achieve compliance *(Security Metrics)*.

When combined with consumers' clear preference for solutions which remove the need for card details to enter an organization's network environment at all, the case for using solutions such as Eckoh's CallGuard to descope the organization's contact center operations from PCI DSS altogether is compelling.

Consumer payment preferences and security expectations

Consumer security perceptions reveal clear preferences

Our research reveals significant consumer concerns about payment security and clear preferences for how organizations should handle payment data.

Persistent agent-related security concerns

Consumer wariness about contact center agents remains a significant barrier to phone-based commerce. 77% of consumers prefer not to give their card details to contact center agents over the phone and 42% view this method of payment as insecure. This persistent concern shows that process-based security approaches have failed to address fundamental consumer anxieties about who is able to access their payment data.

This scepticism directly impacts consumer behavior, with 65% reporting that fraud risk stops them from making payments over the phone, and 75% stating they are reluctant to pay for products or services over the phone due to fraud concerns.

Organizations continue using insecure payment methods

Despite widespread consumer security concerns and available technology alternatives, a significant proportion of organizations continue to rely on the least secure payment method. Our research shows that 25% of consumers were asked to read their card details directly to contact center agents during their most recent phone purchase (rising to 30% of US consumers).

What makes this particularly alarming is the lack of meaningful improvement over time. Our longitudinal research shows that the proportion of consumers being asked to verbally share card details has remained stubbornly stable, at around 23-25% in 2021, 2023 and now 2025, despite escalating fraud levels, heightened consumer awareness of payment security risks.

This disconnect highlights a significant missed opportunity for organizations, as they are not only choosing a payment method that consumers find untrustworthy, but are also maintaining unnecessary compliance overhead while delivering a suboptimal customer experience that 77% of consumers would prefer to avoid.

> ***"We've all experienced it - that point at which you've got to share your information with a complete stranger and you're just hoping that this is not going to lead to your credit card being compromised. But this is front and center for people now, they're so much more aware about data security and data privacy. Maybe a decade ago organizations could get away with less secure approaches because people weren't thinking about data security so much, but that just isn't the case anymore."***
>
> 
> **Nik Philpot**, Eckoh CEO

65%

65% reporting that fraud risk stops them from making payments over the phone

Security perceptions by payment method

Consumer security perceptions reveal a stark divide between technology-mediated and human-mediated payment methods:

Technology-mediated payment methods

Percentage rated as quite or extremely secure

Payment Method	Security Rating
Contactless card payments	**73%**
Online virtual	**72%**
Mobile wallets (e.g. Apple / Android Pay)	**71%**
Average for technology-mediated methods	**72%**

Agent-mediated payment methods

Percentage rated as quite or extremely secure

Payment Method	Security Rating
Webchat with human agent	**47%**
Reading card details to agent	**45%**
Webchat with AI agent	**43%**
Average for agent-mediated methods	**45%**

The 27-percentage point gap between digital and agent-mediated methods demonstrates clear consumer preference for payment technologies that minimize human data handling.

While webchat with AI agents currently rates at 43% for security perception, this figure is remarkably close to human agents (47%) despite being a relatively new technology. More significantly, AI agents are only 2 percentage points behind traditional phone payments where customers read card details directly to human agents (45%), suggesting consumers already view AI as nearly equivalent to established human-mediated payment methods.

As AI technology continues to mature and consumer familiarity grows, AI-enabled payment solutions offer the unique advantage of combining automated efficiency with conversational support that customers often need during payment processes. Combining secure payment processing and AI-powered customer interaction represents the next evolution in contact center excellence, delivering the speed and convenience consumers increasingly expect while preserving human expertise for complex scenarios.

43%
webchat with AI agents currently rates at 43% for security perception

Digital payment method adoption

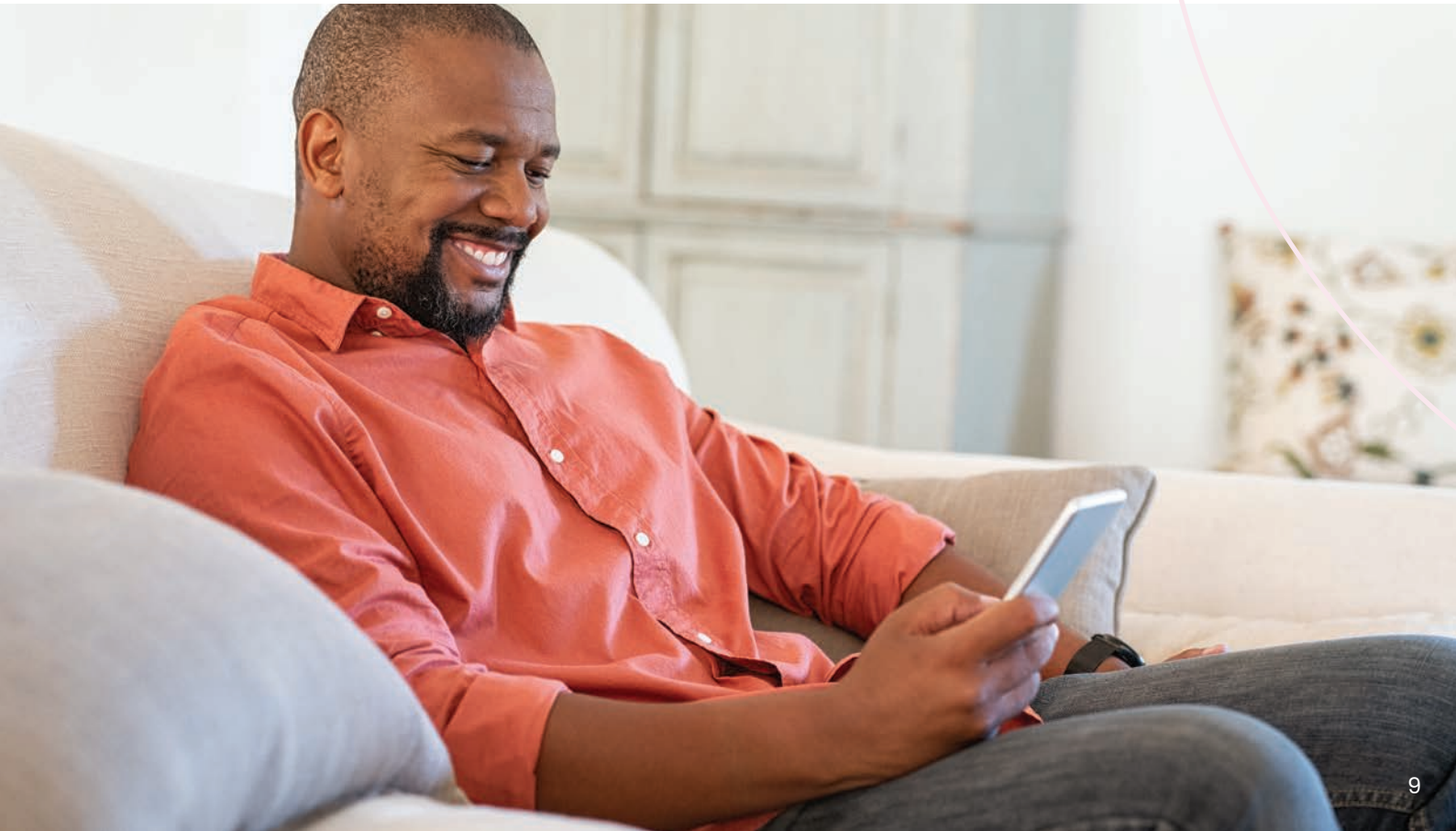
Our survey shows that modern consumers actively engage with diverse payment channels rather than relying on a single preferred method:

- Contactless card payments: 71% have used
- Mobile wallets (*Apple/Android Pay*): 69% have used
- Online virtual systems (*PayPal*): 6% have used

With such high adoption rates across different payment technologies, consumers expect organizations to facilitate omnichannel experiences that allow them to seamlessly choose their preferred payment method depending on context, convenience, and comfort level.

Organizations that fail to provide this breadth of secure payment options risk losing customers who expect the flexibility to pay through their channel of choice, while those that invest in securing multiple payment methods can capture the full spectrum of consumer preferences and build trust across all touchpoints.

> ***"I would say to potential clients: do right by your customers. Show them the respect that they deserve by treating their data sensitively and securely, but also by giving them a better payment experience. Forward-thinking brands want to offer their consumers a payment experience that isn't just secure but is also slicker, more effective, faster and more flexible that they've had before."***
>
>  **Nik Philpot**, Eckoh CEO



Consumer preferences for fraud prevention methods

When asked to identify their preferred fraud prevention method for contact centers, consumer preferences strongly favor technological over process-based approaches:

Payment Method	First Preference
Technology-based solutions (69% combined preference)	
Use secure technology to hide card details from agents	**35%**
Only allow payments via a secure website	**34%**
Process-based solutions (31% combined preference)	
Regular audits and checks on agents	**14%**
Select agents in a 'clean room' environment	**7%**
Remove human agents entirely (use AI)	**6%**
Pause call recordings during payment	**4%**

Despite only 4% of consumers viewing pause-and-resume call recording as their preferred fraud prevention method - by far the least favored approach - many organizations continue to rely on this outdated solution. Organizations persisting with pause-and-resume are not only choosing a method that consumers do not trust but are also maintaining unnecessary PCI compliance overhead and delivering a suboptimal customer experience.

A strategic shift toward de-scoping technologies represents more than just enhanced security; it offers organizations the opportunity to simultaneously reduce costs, eliminate compliance complexity, and deliver the superior customer experience that consumers clearly expect.

> ***"If you know that there is an elegant, effective solution to solve your problem, and you're choosing not to use that, then you're making a decision that essentially means "protecting my customers' data is not my priority". That's pretty scandalous."***
>
>  **Nik Philpot**, Eckoh CEO

45%
45% think AI interaction can resolve issues more quickly

The AI revolution in contact centers

Market growth and adoption trajectories

The AI contact center market demonstrates unprecedented growth, projected to rise from $3.7 billion in 2024 to $19.5 billion by 2034, representing an 18.2% compound annual growth rate (*FMI Globe Newswire, 2025*).

Our survey reveals nuanced consumer attitudes toward AI-powered payment processing. While human agents remain preferred overall, a growing acceptance of AI emerges when security benefits are clearly communicated.

AI capability perceptions

- 42% believe AI agents can provide service quality equivalent to humans
- 45% think AI interaction can resolve issues more quickly
- 52% do not mind whether they deal with an AI or human agent as long as their issues are resolved efficiently

Security-specific AI attitudes

As noted in our key findings, 42% believe AI agents can be more secure than human agents for payment processing. Additionally, 43% report they would worry less about fraud when dealing with AI rather than human agents.

The data suggests substantial opportunity for AI-powered payment solutions, particularly when security advantages are emphasized in customer communications. The fact that over 40% of consumers now view AI agents as potentially more secure than human agents indicates a fundamental shift in perception that organizations can leverage to address the persistent security concerns identified in our research.

60%

60% of consumers like being able to resolve issues without having to speak to anyone

Consumer demand for automated solutions

While our survey reveals some consumer caution about AI agents, deeper analysis of self-service preferences demonstrates clear directional movement toward automated solutions that only AI systems can effectively deliver. The data shows consumers increasingly value the speed, convenience, and consistency that automation provides, but with the safety net of human support when needed:

	Agree	Disagree	Don't know
I like being able to resolve things without having to speak to anyone	**60%**	**33%**	**8%**
I don't mind using self-service as long as I can reach a human agent if I need to	**80%**	**20%**	**0%**
I think virtual agents are improving and becoming more helpful over time	**56%**	**28%**	**17%**
I don't mind whether I'm dealing with an AI agent or a human agent as long as my issue is resolved quickly	**52%**	**40%**	**8%**

This preference pattern indicates that consumer resistance to AI is not fundamentally about the technology itself, but rather about ensuring adequate support when automated systems cannot resolve complex issues.

Perhaps most revealing is that 60% of consumers like being able to resolve issues without having to speak to anyone, demonstrating genuine appetite for fully automated solutions that eliminate human interaction entirely for routine transactions. This preference for autonomous problem resolution aligns perfectly with AI capabilities and suggests that the market is ready for sophisticated automated payment systems that can handle complex inquiries independently, as long as the option to escalate to a human agent remains available.

The human-AI collaboration model

AI use in contact centers does not necessarily mean the wholesale replacement of human agents. Industry trends point toward collaborative models that leverage AI capabilities while maintaining human oversight for complex interactions. This approach addresses consumer preferences while optimizing operational efficiency:

- 71% of Gen Z respondents still view live calls as the quickest way to explain complex issues (*McKinsey, 2025*)
- Complex payment disputes and fraud resolution often require empathy and judgment that only humans can provide (*McKinsey, 2025*)

The optimal model appears to involve AI handling routine payment processing and fraud detection while escalating complex cases to human agents equipped with AI-powered tools and insights.

Consumers want the efficiency and availability that only AI-powered systems can provide - 24/7 accessibility, instant response times, and consistent service quality - while maintaining confidence that human support is available if needed. Importantly, 56% of the consumers we surveyed believe that virtual agents are improving and becoming more helpful over time indicating growing confidence in AI and willingness to embrace enhanced automated capabilities as they become available.

The direction toward hybrid human-AI contact center models may gain significant legislative support if the proposed Keep Call Centers in America Act of 2025 becomes law. This would require businesses to disclose at the outset of any customer service interaction whether the call is being handled by an AI system and, if so, consumers would have the right to request immediate transfer to a human representative physically located in the U.S. if they wished.

Rather than prohibiting AI use, the proposed Act would take a nuanced approach that allows businesses to continue innovating with AI while ensuring consumers maintain control over their interactions. As Senator Gallego, one of the proposers of the bill, noted,

> ***"If someone has a really good experience with an AI bot, there won't be a problem as long as that person knows they're talking to AI versus to a human."***
>
> **CBS News**, 2025

If enacted, this legislative framework would validate the consumer preferences identified in our research and create a strong incentive for organizations to develop AI solutions that genuinely enhance customer experience while maintaining clear human escalation paths.

71%

71% of Gen Z respondents still view live calls as the quickest way to explain complex issues

Younger consumers lead the transformation

Analysis of our survey data by age reveals that the trends identified are significantly more pronounced among younger consumers. This suggests that current preferences among digital natives will increasingly become mainstream expectations as demographic patterns shift over time.

AI security confidence shows strong generational divide

When examining levels of agreement with the statement "AI agents can be more secure than human agents", younger consumers demonstrate markedly higher confidence levels. Consumers under 45 show 50% agreement compared to just 29% for those over 45, a substantial 21 percentage point gap. This finding is particularly significant as it indicates that security-focused AI adoption will gain momentum as younger, more AI-confident consumers represent larger market segments.

Autonomous service preference highest in peak earning years

The preference for autonomous problem resolution follows an interesting pattern, with the strongest preference among consumers aged 35-44 (72.5% agreement), followed by 25–34-year-olds (64%). Overall, consumers under 45 show 65% preference for autonomous service compared to 50% for those over 45 - a 15-percentage point difference. This pattern suggests that professionals in their peak earning and decision-making years are driving demand for efficient, autonomous payment solutions.

Strategic implications of generational data

These generational differences provide compelling evidence that the trends toward AI-powered secure payment solutions are not temporary preferences but indicators of long-term market evolution. Organizations that position themselves ahead of this demographic shift will establish competitive advantages that strengthen over time. The data suggests that investment in AI-enhanced payment security represents preparation for inevitable market transformation rather than speculative innovation.

72.5%

72.5% of consumers aged 35–44 show the strongest preference for solving problems independently

74%
74% of US consumers indicating easier and faster checkouts as primary reasons for digital payment adoption

Omnichannel payment expectations

The seamless experience imperative

Consumer expectations for payment experiences have evolved to demand consistency across all interaction channels. Omnichannel customers spend 30% more than single-channel shoppers, while brands with strong omnichannel strategies see 9.5% annual revenue increases compared to 3.4% for weak strategies (*Firework, 2025*), so companies ignore these trends at their peril.

Our survey confirms these expectations through payment method adoption patterns. High usage rates across multiple payment technologies indicate consumer comfort with diverse payment approaches, provided security standards remain consistent. The challenge for organizations is delivering unified security experiences across channels while accommodating varied consumer preferences.

Consumers no longer view security and convenience as trade-offs. Instead, both have become core requirements for digital payment methods, with 74% of US consumers indicating easier and faster checkouts as primary reasons for digital payment adoption (*McKinsey, 2024*).

This evolution creates opportunity for payment security solutions that enhance rather than complicate the customer experience. Technologies that remove friction while improving security, such as automated payment processing that eliminates the need to verbally share card details, align with both consumer preferences and business objectives.

Payment security as customer experience strategy

Security as experience differentiation

Organizations have traditionally approached payment security from a risk management and compliance perspective, viewing investments in security as necessary costs rather than strategic advantages. However, our research reveals a fundamental shift in how payment security impacts customer experience and competitive positioning. The convergence of heightened consumer security awareness, demand for seamless automated experiences, and AI capabilities creates unprecedented opportunity for organizations to transform payment security from a compliance burden into a customer experience differentiator.

The evidence for this transformation is compelling. When 82% of consumers report growing concern about payment card fraud and 77% prefer not to provide card details directly to agents, it is clear that security concerns directly influence customer willingness to complete transactions. Organizations that can demonstrably remove payment data from agent environments while maintaining service quality address both security concerns and experience expectations simultaneously. This dual benefit creates competitive advantage that extends far beyond regulatory compliance.

The experience-security convergence

Consider the customer journey implications: traditional phone payment processes require customers to verbally share sensitive card details with agents, creating friction through security anxiety, potential misunderstandings, and extended transaction times. De-scoping technologies that remove payment data from contact center environments address these pain points by enabling customers to complete transactions through secure automated systems while maintaining agent support. This delivers the dual benefit of enhanced security and improved customer experience.

The competitive differentiation extends beyond individual transactions. Organizations that implement comprehensive secure payment solutions signal to customers that they prioritize data protection and understand modern consumer expectations.

> ***"The payment process with Eckoh's solution is so much slicker, so much more effective, and so much faster than the traditional way. Your agents are going to be occupied for less time. Your customer experience is better and they can choose their preferred payment method. Card data is completely protected. There are literally no downsides - that's what's so extraordinary. Organizations need to be more honest with themselves about the cost and overhead of the traditional things they might be doing to try and protect the data and get through their PCI audit every year, all of which is just simply washed away by engaging with Eckoh."***
>
> 
> **Nik Philpot**, Eckoh CEO

Strategic repositioning of security investment

Our research suggests organizations should fundamentally reframe payment security investments. Rather than viewing them solely through compliance and risk reduction lenses, payment security technologies should be evaluated for their contribution to the organization's bottom line.

The 80% of customers who will abandon brands after negative experiences (*Wiser Notify, 2024*) includes those who experience payment security anxiety or fraud. Comprehensive security measures protect against both actual fraud and the perception of vulnerability that drives customer defection.

AI-powered secure payment systems simultaneously improve security, reduce compliance costs, and enhance service delivery speed and consistency. The 56% of our survey respondents who believe virtual agents are improving over time represent growing market acceptance of AI-enhanced service experiences.

The message is clear: payment security and AI adoption should be strategic initiatives that enhance competitive positioning and customer relationships, not merely tactical responses to compliance requirements. Organizations that recognize and act on this opportunity will establish advantages that compound over time as consumer expectations continue evolving toward secure, automated and seamless payment experiences.

80%

80% of customers abandon brands after negative experiences, including issues like payment security concerns or fraud

Conclusion

The payment security landscape has undergone fundamental transformation since our 2023 research, driven by regulatory evolution, escalating fraud threats, and rapid AI adoption. Our comparative analysis reveals both concerning trends and significant opportunities that organizations must address strategically.

The continued erosion in consumer confidence represents a critical challenge that cannot be ignored. Traditional security approaches fail to meet consumer expectations and evolving threat realities. Consumers' preference for technology-based security solutions is clear, providing clear market validation for continued investment in solutions that remove payment data from human-mediated processes.

Organizations face a strategic choice: invest in comprehensive payment security technologies that address the declining trust trends or continue managing increasing compliance costs while risking further customer defection due to persistent security concerns.

The evidence strongly supports integrated approaches that combine AI-enhanced customer experiences with robust security measures. Technologies that remove payment data from contact center environments entirely address multiple challenges simultaneously: they restore consumer confidence, eliminate the PCI DSS compliance burden, reduce fraud risk, and enable the AI-powered service improvements that consumers increasingly expect.

Organizations that embrace comprehensive transformation of their payment security capabilities will be best positioned for success in the evolving payments landscape, while those that continue with incremental approaches risk further erosion of customer trust and competitive position.

How Eckoh addresses these challenges

Eckoh's secure payment solutions directly address every consumer concern and market challenge identified in this research. Our technology ensures that payment card data never enters contact center environments or is shared with an agent, addressing the 77% of consumers who prefer not to provide card details verbally to agents and the 69% who favor technological over process-based security approaches.

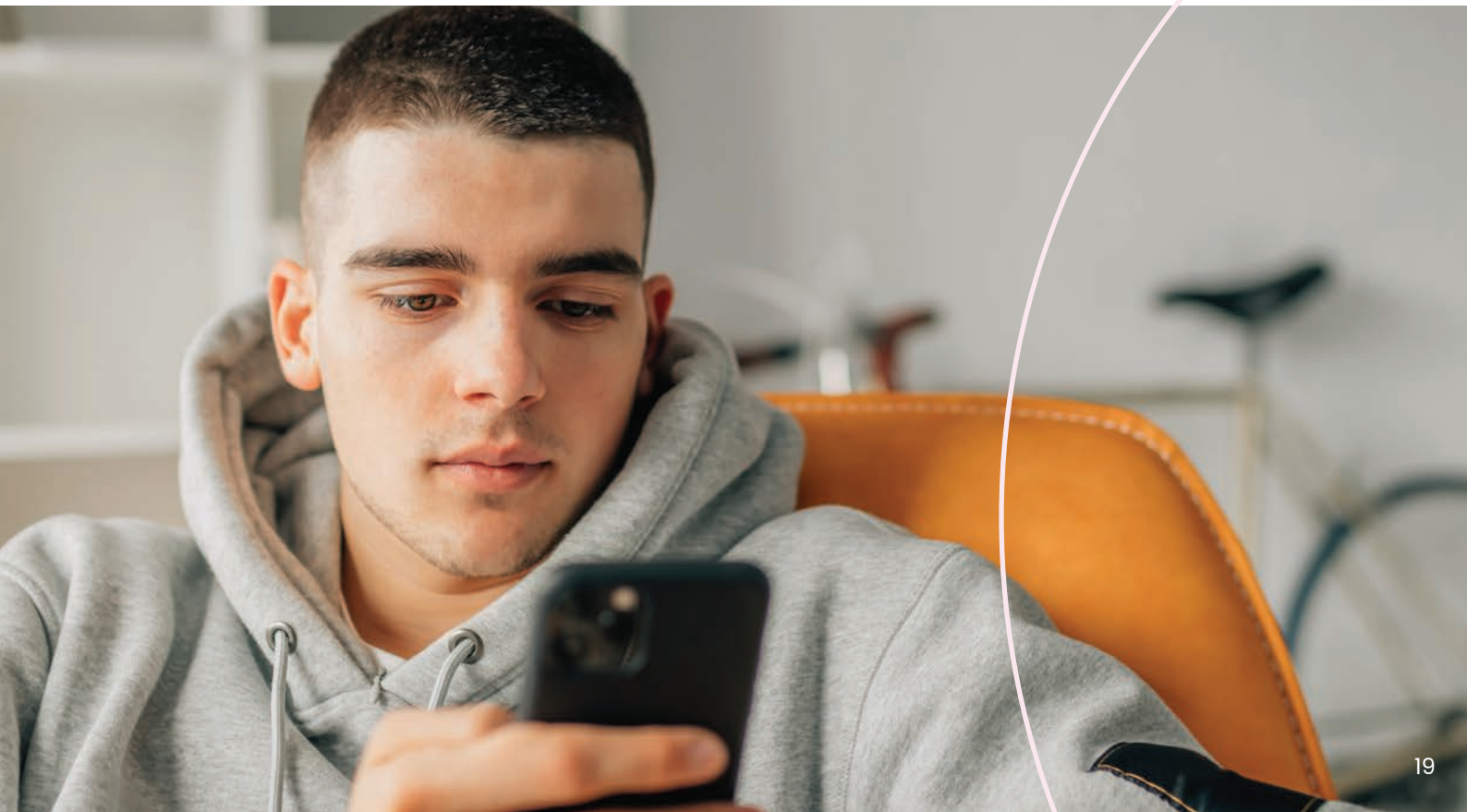
By enabling customers to enter their payment details via telephone keypad or secure digital channels while agents remain connected to provide support, Eckoh delivers the secure, technology-mediated experience that consumers rate 27 percentage points higher for security than traditional agent-mediated methods.

The comprehensive de-scoping approach eliminates the burden of PCI DSS compliance, saving organizations the cost of ongoing audits, remediation and infrastructure maintenance, while removing the operational complexity of securing payment data.

Eckoh's solutions also position organizations for the AI-enhanced future that many consumers now view as potentially more secure than human agents. Our secure payment technology also integrates seamlessly with AI-powered contact centers, enabling the human-AI collaboration model that consumers prefer, combining automated efficiency for routine payment processing with human expertise for complex customer service needs.

Whether organizations are implementing AI gradually or maintaining traditional contact centers, Eckoh's secure payment technology ensures consistent security standards across all channels while delivering the superior customer experience that builds trust, reduces fraud risk and creates competitive advantage in an increasingly security-conscious market.

To discover how Eckoh can transform your payment security from a compliance burden into a competitive advantage, contact our team today at www.eckoh.com.



References

1. CBS News (2025). "New bill aims to protect American call center jobs and consumers from AI". July 30, 2025. Available at https://www.cbsnews.com/news/keep-call-centers-in-america-act-artificial-intelligence/
2. Firework. (2025). "52+ Omnichannel Stats You Can't Afford to Ignore in 2024 (Or Risk Losing Customers!)." March 11, 2025. Available at: https://firework.com/blog/omnichannel-statistics
3. McKinsey. (2024). "State of consumer digital payments in 2024." October 25, 2024. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/state-of-consumer-digital-payments-in-2024
4. McKinsey. (2025). "The right mix of humans and AI in contact centers." March 19, 2025. Available at: https://www.mckinsey.com/capabilities/operations/our-insights/the-contact-center-crossroads-finding-the-right-mix-of-humans-and-ai
5. Merchant Cost Consulting. (2025). "Credit Card Fraud Statistics (2025)." February 19, 2025. Available at: https://merchantcostconsulting.com/lower-credit-card-processing-fees/credit-card-fraud-statistics/
6. PCI Security Standards Council. (2024). "Just Published: PCI DSS v4.0.1." Available at: https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1
7. PCI Security Standards Council. "PCI Data Storage Do's and Don't's". Available at https://listings.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf
8. PCI Security Standards Council. (2023). "Securing the Future of Payments: PCI SSC Publishes PCI Data Security Standard v4.0." September 28, 2023. Available at: https://www.pcisecuritystandards.org/about_us/press_releases/securing-the-future-of-payments-pci-ssc-publishes-pci-data-security-standard-v4-0/
9. Qualtrics. (2024). "Contact Center Trends 2025." December 9, 2024. Available at: https://www.qualtrics.com/blog/contact-center-trends/
10. Recorded Future. (2024). "2024 Payment Fraud Report: Trends, Insights, and Predictions for 2025." Available at: https://www.recordedfuture.com/research/annual-payment-fraud-intelligence-report-2024
11. Securitymetrics.com. "How much does PCI compliance cost?". Available at https://www.securitymetrics.com/blog/how-much-does-pci-compliance-cost
12. Security.org. (2025). "62 Million Americans Experienced Credit Card Fraud Last Year." January 27, 2025. Available at: https://www.security.org/digital-safety/credit-card-fraud-report/
13. Wiser Notify. (2024). "45 Omnichannel Statistics & Trends (New 2025 Data)." December 19, 2024. Available at: https://wisernotify.com/blog/omnichannel-stats/

This report continues Eckoh's commitment to providing industry-leading insights into payment security trends and consumer behavior. For more information about how Eckoh's secure payment solutions can help your organization address these evolving challenges and opportunities, visit www.eckoh.com.

Eckoh

Build a trusted self-service solution today

To learn more about building a secure self-service solution for your call center, please contact us to book a demo.

Book a demo