2025 TECH TRENDS REPORT • 18TH EDITION

FINANCIAL SERVICES & INSURANCE

FTSG

Future Today Strategy Group's 2025 Tech Trend Report

Our 2025 edition includes 1000 pages, with hundreds of trends published individually in 15 volumes and as one comprehensive report. Download all sections of Future Today Strategy Group's 2025 Tech Trends report at **www.ftsg.com/trends.**

Nick Bartlett
Financial Services
and Insurance Lead

Transformation efforts need to happen now—before it's too late.

The next decade will be make-or-break for companies in the financial services and insurance industry based on their ability to harness the immense amount of data available to improve efficiency, personalization, and speed. While headlines focus on the latest artificial intelligence breakthroughs, a more fundamental challenge looms larger: the capacity to build and maintain the data and computing infrastructure necessary to support these advancements at an unprecedented scale. While many companies have made strides in modernization, they're moving too slowly compared to the rapid pace of technological change. Current efforts, though commendable, risk falling short of the rapid advancements in the tech sector. By 2030, this industry will face significant disruption from nontraditional competitors that are already integrating sophisticated financial and insurance capabilities into their offerings. To maintain industry leadership, companies must accelerate digital transformation efforts and embrace cutting-edge technologies more comprehensively.

The transformation needed in financial institutions isn't just about upgrading systems; it demands a fundamental reimagining of operational models that will determine their relevance in the evolving financial landscape. The industry faces significant challenges—from the substantial computational demands of AI workloads to the widening skills gap in specialized infrastructure management and growing data privacy concerns—yet these hurdles also present unprecedented opportunities. Companies that successfully modernize their platforms with a focus on business strategy rather than technology alone stand to gain improved customer experiences, enhanced data analytics capabilities, and greater regulatory agility. Building robust, scalable, and secure computing infrastructures will help companies maintain a competitive advantage and control of their own destiny in an increasingly digital financial world. The institutions that rise to the occasion will lead in AI adoption and actively shape the future of finance, securing their place at the forefront of the industry's next evolution.

Forward-thinking institutions that embrace comprehensive digital transformation now will be best positioned to lead as the industry becomes evermore technology-driven. The future of financial services is being written today, and it will be defined by those who take decisive, strategic action to modernize their operations and capabilities.

Regulatory adaptation and scrutiny will underscore transformative efforts over the next year.

1

AI Governance Is a Strategic Imperative

The NAIC's AI model bulletin, adopted by 21 states, signals intensifying regulatory scrutiny of AI in financial services and calls for robust governance frameworks.

2

Quantum Computing Will Revolutionize Future Risk Modeling

Banks like Citi are already experimenting with quantum computing for portfolio optimization and fraud detection, heralding a new era in financial management.

3

Digital Identity Is the New Battleground for Data Security

With digital wallets projected to reach 5.2 billion users by 2026, securing digital identities becomes crucial in preventing fraud and protecting sensitive financial data.

4

Climate Change Is Redefining Risk Management

Swiss Re estimates that climate risks could reduce global GDP by 11%–14% by 2050, forcing insurers and banks to radically rethink their risk assessment models.

5

Instant Payments Are Accelerating Disruption of Legacy Systems

The EU's mandate for instant payments and the success of Brazil's Pix system are driving global adoption of real-time payment infrastructure.

A perfect storm of forces are rapidly reshaping financial services and insurance.

The financial services industry is undergoing a profound transformation, marked by forces that create both extraordinary opportunities and systemic risks. AI has evolved from theoretical applications to become foundational technology, now powering core operations, from underwriting and fraud detection to customer service and risk modeling. However, its rapid deployment across the industry requires robust governance frameworks to prevent bias and ensure equitable outcomes.

Real-time interactions have become the baseline expectation across financial services. Instant payments, driven by regulatory mandates and consumer demand, are positioned to replace legacy systems. This shift creates a hyperefficient transactional landscape while introducing new vulnerabilities that call for sophisticated security measures. Similarly, digital identity has evolved beyond basic authentication into a complex ecosystem of personal data and financial credentials, magnifying the importance of data privacy and cybersecurity.

The insurance sector faces mounting challenges as climate-related disasters increase in frequency and severity, necessitating new risk models and coverage strategies to address escalating losses and maintain long-term solvency. Simultaneously, widespread digitalization exposes institutions to increasingly sophisticated cyberthreats, and they'll need to shift from reactive security to proactive, intelligence-driven defense architectures.

The decisions made in this period of transformation will shape not only individual institutions but the stability and inclusivity of the entire financial ecosystem. This convergence of technological advancement, changing consumer expectations, and emerging risks defines the current state of financial services and sets the stage for its evolution.

Artificial intelligence is a top focus, prompting new product rollouts and several regulatory changes.

MAY 2024

Key Players Form AI Readiness Working Group

The Fintech Open Source Foundation's new task force is developing a governance framework for safe AI implementation.

JULY 2024

NY Dept of Financial Services Issues AI Circular

The guidance regulates NY-based companies in their use of artificial intelligence in insurance underwriting and pricing.

SEPTEMBER 2024

JPMorgan Chase Launches AI Assistant

Chase introduces the AI assistant LLM Suite to more than 140,000 employees, just one piece of a broader AI strategy.

OCTOBER 2024

AXA XL Launches AI Coverage

The new endorsement to AXA XL's cyber policies covers data poisoning, usage rights infringement, and regulatory violations.

DECEMBER 2024

States Adopt NAIC's AI Guidance

By the end of 2024, 21 states had adopted the NAIC's Model Bulletin on the Use of AI Systems by Insurers.

« PAST

Decreasing US regulation and oversight could reshape the industry.

Q1–Q2 2025

Capital One Moves Cards to Discover Rails

Following a successful acquisition, Capital One plans to move its cardholders over to the Discover network.

Q2–Q3 2025

Bank M&A to Become Easier and Faster

The Trump administration has promised deregulation, and the industry is gearing up for streamlined deal approvals.

Q4 2025–Q1 2026

Truth.Fi's Disruptive Fintech Offerings

Trump's fintech venture Truth.Fi recently announced plans to offer customized ETFs and cryptocurrency products in the future.

FUTURE »

Q2 2025

Basel III Endgame in Question

With Donald Trump in and Michael Barr out, the Fed's Basel III regulations are in limbo, potentially easing banks' capital requirements.

Q2–Q4 2025

Insurer Response to Climate Crisis

As insurers reel from wildfire losses earlier in the year, watch for policy and coverage changes.

AI and decentralization are transforming the future of financial services.

Hyper–Personalized Risk Ecosystems

AI-driven data modeling will transform risk assessment by creating dynamic, individualized financial profiles that transcend traditional credit scoring, enabling institutions to make nuanced decisions based on holistic, real-time behavioral insights and alternative data streams.

Programmable Value Networks

Cryptocurrency and open banking could plausibly converge to create fluid, borderless financial ecosystems where value transfer becomes instantaneous, programmable, and decentralized, fundamentally reimagining how capital moves across global economic landscapes.

Autonomous Compliance Engines

Advanced AI and blockchain technologies will create self-regulating compliance mechanisms that dynamically adapt to evolving regulatory landscapes, reducing human error and transforming risk management from a reactive to a predictive discipline.

Parametric Risk Intelligence

AI-powered parametric insurance models will revolutionize risk transfer by enabling instantaneous, algorithmically triggered protection mechanisms that respond to predefined environmental, technological, and economic parameters with unprecedented precision.

Frictionless Identity Economics

Digital identity technologies will emerge as the foundational infrastructure for a new economic paradigm, where authentication becomes seamless, privacy-preserving, and cryptographically secure across financial, governmental, and commercial interactions.

Cyber Resilience Architectures

Emerging cyber risk mitigation strategies will transform from defensive postures to proactive, intelligence-driven ecosystems that anticipate, neutralize, and learn from potential threats through advanced machine learning and predictive analytics.

These individuals are at the forefront of development and transformation in the financial services & insurance industry.

- **Andrew Mais, Connecticut's insurance commissioner,** for his work on the potential of AI and the importance of regulatory compliance.
- **Brian Collins, executive director of the Earth Fire Alliance,** for his organization's work to build a satellite constellation focused specifically on fire, ushering in a new era of fire monitoring.
- **Dave Jones, director of the Climate Risk Initiative at University of California, Berkeley,** for his founding of the Sustainable Insurance Forum and forward-thinking work on climate impacts to insurance.
- **Günther Thallinger, board member of Allianz SE and chair of the UN Net-Zero Asset Owner Alliance,** for his work leading sustainable finance initiatives and aligning global investment portfolios with net-zero goals.
- **Dr. Henna Karna, Harvard fellow and formerly from Google,** AXA, AIG, and Verisk, for her work on the impact of AI on the insurance workforce, including the need for AI literacy and talent development.
- **Dr. Marco Pistoia, head of Global Technology Applied Research at JPMorgan Chase,** for his research in the application of quantum, blockchain, and other technologies in the field of financial services.
- **Rafael Forte Araújo Cavalcanti, SVP data, analytics and AI at Bradesco,** for his work developing generative AI use cases for banking in the Bradesco Artificial Intelligence Lab.
- **Dr. Robert Hartwig, director, Risk and Uncertainty Management Center, and clinical associate professor at University of South Carolina,** for his ongoing thought leadership and research on the insurance market.
- **Rose Goslinga, co-founder and CEO of Pula,** for her work pioneering climate insurance and risk management solutions for smallholder farmers in emerging markets.
- **Ryan Bank, founder and global managing director of the Geospatial Insurance Consortium,** for his work broadening aerial imagery for the insurance sector.
- **Serge Beck, CEO and founder of Omniwire,** for his work to develop more secure financial systems for consumers.
- **Sopnendu Mohanty, chief fintech officer of the Monetary Authority of Singapore,** for his work driving fintech innovation and regulatory frameworks that foster digital finance and insurtech.

Advancing technology will drive increased revenues and decreased expenses...

OPPORTUNITIES

Ecosystem Orchestration

Open banking can help institutions integrate diverse services and create value-added ecosystems. Through cross-sector partnerships, banks can enhance engagement and generate new revenue.

Behavioral Economics Integration

AI-driven insights will enable firms to nudge customers toward better decisions. By analyzing patterns in spending, saving, and investing, institutions can design personalized offerings that improve financial health while fostering stronger customer relationships.

Embedded Finance Proliferation

Financial services are seamlessly integrating into nonfinancial platforms. These strategic partnerships allow firms to offer new products to new customers, securing relevance in an increasingly platform-driven economy.

Regulatory Technology (RegTech) Leadership

Firms pioneering AI-driven compliance solutions will gain a competitive advantage. By developing sophisticated RegTech capabilities, they can automate compliance processes, predict regulatory changes, and proactively manage risk.

...but firms must navigate rapidly evolving digital and compliance risks.

THREATS

Data Sovereignty Challenges

The proliferation of localized data laws may complicate cross-border services and data management strategies. Institutions must steer through a complex web of regulations that potentially require duplicative infrastructure and increasing operational costs.

Digital Identity Monopolies

Tech giants may dominate digital identity verification, marginalizing traditional financial institutions in customer relationships. As these platforms become primary gatekeepers of identity, banks and insurers risk losing direct customer engagement and valuable insights.

Quantum Computing Encryption

Quantum advancements could render current cryptographic methods obsolete, necessitating rapid and costly security overhauls. Institutions face the task of quantum-proofing their entire digital infrastructure to prevent unprecedented security risks and maintain customer trust.

Climate Liability Exposure

Insurers face potential litigation for underestimating climate risks that could lead to unforeseen liabilities and reputational damage. As climate-related events intensify, insurers may be held accountable, resulting in financial losses, regulatory scrutiny, and erosion of public trust.

The right strategies will guide financial leaders through the emerging landscape.

Implement solutions, such as blockchain-based capabilities, for smart contracts, instant payments, and secure digital identity verification. This will streamline operations, reduce fraud, and enable new business models in areas such as parametric insurance and decentralized finance.

Establish comprehensive digital literacy programs and data science training initiatives for existing staff, while also recruiting specialists in emerging fields like climate risk modeling and behavioral economics to ensure the workforce can leverage new technologies effectively.

Proactively engage with regulators to shape policies around open banking, data privacy, and digital currencies. By participating in regulatory sandboxes and industry working groups, companies can help create a balanced regulatory environment that fosters innovation while protecting consumers.

Allocate significant resources to develop a robust cybersecurity infrastructure, including advanced encryption capabilities. This investment will safeguard against evolving cyberthreats, protect sensitive customer data, and maintain trust in an increasingly digital financial ecosystem.

Develop integrated platforms that leverage open banking APIs and alternative data sources for enhanced credit scoring and risk assessment. This will enable more accurate underwriting, personalized product offerings, and improved access to financial services for a broader market.

Invest in climate risk modeling tools and sustainable finance initiatives. This will help insurers better assess and price climate-related risks, while enabling financial institutions to develop innovative green financial products that align with global sustainability goals.

Technology Deployment

Capital Expenditure

Talent Development

Regulatory Influence

FINANCIAL SERVICES & INSURANCE TRENDS

BUILDING BLOCKS

12TH YEAR ON THE LIST

DIGITAL IDENTITY

WHAT IT IS

Digital identity is evolving rapidly, driven by increased digital interactions, regulations, and technological advancements. By 2026, a significant transformation in how individuals control and protect their digital identities will reshape security, privacy, and accessibility.

HOW IT WORKS

Digital identity is the unique representation of an individual, organization, or device in the digital space. It comprises identifiable attributes like usernames, passwords, biometric data, and other personal information for online interactions and transactions. The concept of digital identity has existed since the early days of the internet, but its significance has dramatically increased as our lives have become more digitally integrated.

Creating and managing digital identities involves complex systems that collect, verify, and store personal data. For example, when setting up a new online account, a user provides information such as an email address, password, and sometimes biometric data like fingerprints or facial recognition. The service provider then authenticates this data, to create a digital identity profile.

Increasingly, governments are also exploring digital identities. Last year, Australia's Parliament passed the Digital ID Bill 2024; it lays the groundwork for a nationwide digital identity system that allows financial institutions and service providers to integrate with the government's Digital ID platform, enhancing security and convenience for users. Similarly, the US Department of Commerce's National Institute of Standards and Technology is working to adapt digital identity guidelines to support public benefits programs.

WHY IT MATTERS

Adopting digital identity systems offers vital benefits, including fraud prevention and improved security for personal information. As seen with Australia's new law, the systems can be regulated to protect users by ensuring that only accredited service providers can handle digital identities, thereby reducing the risk of fraud and identity theft.

Another critical aspect is accessibility. Digital identity systems can provide official documentation to individuals who previously lacked it, such as refugees or people living in remote areas, improving their access to essential services. This is particularly evident in initiatives like those supported by the UN Refugee Agency, which integrates refugees into national identification systems across several African nations.

Digital identity also offers individuals greater control over their personal information. For instance, Japan's major banks are working on a digital identity solution that allows users to store their data on their mobile devices securely, giving them complete control over their information. But the widespread adoption of digital identities also presents challenges. As more personal information is stored online, the potential for breaches increases, necessitating robust security measures and requiring a delicate balance between convenience and privacy.

7TH YEAR ON THE LIST

SCALING CRYPTO-CURRENCIES

WHAT IT IS

Regulatory approval of cryptocurrency products like Bitcoin ETFs is transforming the market by bringing digital assets into the realm of traditional finance. This shift is fostering broader adoption, institutional engagement, and a more stable market environment.

HOW IT WORKS

In 2024, the cryptocurrency market underwent a significant transformation driven by regulatory advancements and institutional integration. One of the most impactful developments was the US Securities and Exchange Commission's approval of Bitcoin exchange-traded funds. These ETFs allow investors to purchase shares in a fund that holds Bitcoin and trades on regulated exchanges like Nasdaq, marking the first time cryptocurrencies have been brought under the same regulatory umbrella as other financial instruments. Soon after, the UK's Financial Conduct Authority approved crypto-backed exchange-traded notes for professional investors. The introduction of Bitcoin ETFs represents a broader trend toward the institutionalization of cryptocurrencies, but as of January, the US stopped short on full institutionalization after the incoming administration promptly banned a US CBDC (or digital dollar).

Major financial institutions and payment processors are increasingly offering cryptocurrency services, further embedding digital assets into the traditional financial system. For instance, Stripe, a leading fintech company, has reentered the cryptocurrency space by allowing merchants to accept payments in stablecoins like USDC on multiple blockchains. This is the first time Stripe has accepted cryptocurrencies since 2018. This move signifies a shift in the perception of digital currencies, recognizing them as viable means of everyday transactions rather than merely speculative assets.

WHY IT MATTERS

As regulatory frameworks solidify, the cryptocurrency market is becoming more accessible and less volatile, attracting a more diverse and risk-averse investor base. The approval of Bitcoin ETFs and the increasing integration of cryptocurrencies into traditional financial services mark the beginning of a new era for digital assets. These regulatory developments legitimize cryptocurrencies and pave the way for more institutional investment, which is crucial for the market's long-term stability and growth.

However, the move toward greater regulation also brings new challenges. As governments and regulatory bodies like the SEC continue to develop and enforce cryptocurrency regulations, the industry will need to adapt to new compliance standards. This could include stricter Know Your Customer and Anti-Money Laundering requirements, which may increase operational costs for crypto exchanges and other service providers. Another challenge will likely be a more fragmented and complex global regulatory environment as more countries follow US efforts to regulate digital assets.

For businesses, the implications are profound. Companies that can navigate this evolving regulatory landscape will be well-positioned to capitalize on the growing acceptance of cryptocurrencies. On the other hand, those that fail to comply with new regulations could face significant legal and financial repercussions.

3RD YEAR ON THE LIST

OPEN BANKING

WHAT IT IS

In 2024, US banks faced a turning point when the Consumer Financial Protection Bureau (CFPB) advanced its rule on "personal financial data rights," pushing them to adopt open banking or risk losing ground. The rapid integration of open banking APIs is now critical for staying competitive.

HOW IT WORKS

Open banking has been driven by mandates like the European Union's second Payment Services Directive (PSD2) and the UK's Open Banking Standard. The CFPB advanced similar regulations under its 2024 rule mandating the secure sharing of consumer financial data.

Key players continue to expand, enabling a new generation of services. Plaid connects with more than 11,000 financial institutions, allowing applications like Venmo, Robinhood, and Coinbase to securely access and use financial data to offer seamless digital financial services. Stripe also launched a new open banking–powered payment method, "Pay by Bank," in the UK so that businesses can accept bank-to-bank payments without the need for credit cards, as a more secure and cost-effective payment option. Similarly, Klarna, a Swedish payments fintech company, has introduced open banking–powered settlement services in Europe for users to make direct payments from their bank accounts rather than use traditional payment cards.

For small and medium-size enterprises, open banking enables better cash flow management through real-time access to financial data and integration with accounting software. This streamlining allows businesses to make informed financial decisions, optimize working capital, and reduce the cost of financial operations.

WHY IT MATTERS

The competitive landscape is rapidly shifting as fintech companies and new market entrants leverage open banking to introduce innovative financial solutions that directly challenge traditional players. For example, Revolut and Monzo, two digital-only banks, have capitalized on open banking to offer services like budgeting tools, real-time spending notifications, and no-fee foreign transactions. Traditional banks and insurance companies must adapt by forming partnerships with these agile fintechs or developing their own competitive offerings. By integrating open banking solutions, they can expand their service portfolio, reach new customer segments, and capture a larger market share.

Operational efficiency and compliance are also crucial considerations. Open banking enables seamless integration across various financial platforms, reducing the need for manual processes and minimizing the risk of human error. This integration can lead to significant cost savings, particularly in areas like payment processing and customer onboarding.

As regulatory frameworks become more stringent, financial institutions that are proactive in adopting secure and compliant open banking practices will mitigate regulatory risks and avoid potential fines. Additionally, the enhanced data visibility provided by open banking can improve fraud detection capabilities, allowing institutions to better protect their customers and reduce the risk of financial loss.

2ND YEAR ON THE LIST

AI-ASSISTED DATA MODELING

WHAT IT IS

AI-assisted data modeling is transforming industries like finance and insurance by enhancing risk management, fraud detection, and decision-making. Major players like Visa and Lemonade are leveraging AI to improve operational efficiency, reduce fraud, and drive competitive advantage.

HOW IT WORKS

AI-assisted data modeling utilizes artificial intelligence to analyze vast amounts of data, uncover patterns, and make predictions that inform business decisions. This technology has significant applications in industries like finance and insurance, where companies deal with large volumes of complex data.

Visa integrated AI into its fraud detection systems, using a range of AI-powered tools to assess transaction risks in real time. These tools analyze data from multiple sources, apply machine learning models to detect anomalies, and assign risk scores to each transaction. Similarly, digital insurance company Lemonade has developed a suite of AI models, including a composite AI called LTV, which aggregates insights from 50 different machine learning models to predict the lifetime value of each customer. This allows Lemonade to make more informed decisions about customer acquisition and retention strategies, ultimately improving its loss ratio—a key measure of an insurance company's efficiency.

AI models in these contexts work by being trained on historical data, learning from past transactions, and continuously updating their algorithms as new data becomes available. These systems can then identify patterns that human analysts might miss, such as subtle shifts in customer behavior or emerging fraud tactics. The AI's ability to process and analyze data at scale enables businesses to make real-time decisions that improve efficiency and reduce risk.

WHY IT MATTERS

The integration of AI into data modeling represents a significant shift in how industries manage risk and make decisions. For financial services and insurance, where the ability to accurately assess risk is crucial, AI provides a competitive edge by enhancing the accuracy and speed of decision-making processes. For instance, AI models can predict the likelihood of fraud far more effectively than traditional methods, making companies more proactive in being able to prevent fraudulent transactions. This not only saves money but also enhances customer trust and satisfaction. These AI-assisted models can also improve customer segmentation and personalized marketing, helping companies to better target their services and improve customer retention.

The impact of AI-assisted data modeling is profound, especially as the technology continues to evolve. With AI, companies can harness vast amounts of data to drive more strategic decision-making, improve operational efficiency, and maintain a competitive advantage in an increasingly data-driven world. But the adoption of AI also brings challenges, such as the need for robust data governance and the potential for new forms of cyberthreats. As AI models become more sophisticated, the risk of adversarial attacks—where bad actors manipulate AI systems—also increases. Organizations must invest in securing their AI systems and ensuring that they are transparent and accountable.

SCENARIO YEAR 2040

SYNTHETIC OVERLOAD

By 2035, financial institutions and insurers have fully transitioned to digital-first operations. Physical branches are obsolete, replaced by AI-powered virtual service hubs that handle onboarding, claims, and transactions remotely. Biometric verification and video KYC (Know Your Customer) protocols are standard, offering convenience and efficiency. However, these advancements inadvertently create fertile ground for a new threat: hyper-realistic synthetic identities. Generative AI has evolved to produce “Super Synthetic Identities,” blending stolen personal data with AI-generated biometrics, deepfake videos, and fabricated behavioral patterns. These identities are indistinguishable from real individuals, bypassing even the most advanced verification systems. Fraudsters exploit this technology to secure loans, file insurance claims, and conduct financial transactions on a massive scale.

For several years, the financial system is thrown into chaos as synthetic identity fraud spirals out of control. Insurers face skyrocketing fraudulent claims supported by deepfake accident footage and fabricated medical records, driving up loss ratios and premiums. Banks are inundated with defaults on loans issued to nonexistent customers. Trust in the financial system erodes as legitimate customers bear the cost of rising fraud. Regulators step in, mandating the adoption of cryptographic identity systems tied to government-issued digital credentials.

In 2040, a global “Digital Trust Initiative” emerges, albeit fragmented by region, requiring all digital interactions to be verified through secure hardware-based cryptographic keys combined with live biometric authentication. While this restores some stability, it comes at the cost of increased surveillance and reduced privacy. The financial system survives, but society is left grappling with the trade-offs between security and freedom in an era dominated by synthetic deception.

SEAMLESS INTERACTIONS

6TH YEAR ON THE LIST

PROGRAMMABLE MONEY

WHAT IT IS

Programmable payments are transactions that execute automatically based on predefined conditions. Central banks and financial institutions are accelerating their adoption of programmable money, enabling rule-based transactions that enhance efficiency, security, and financial inclusion.

HOW IT WORKS

Unlike traditional money, which often requires manual intervention or third-party oversight, programmable money enforces rules at the transaction level, ensuring funds are used as intended without intermediaries.

India's e-rupee, a blockchain-based central bank digital currency (CBDC), is set to expand cross-border transactions and programmable money applications in 2025. The Reserve Bank of India (RBI) is working to integrate the e-rupee with the Unified Payments Interface, potentially driving mass adoption by linking it to India's well-established digital payment ecosystem. To enhance public understanding and trust, the RBI held in-person CBDC training sessions in New Delhi in February 2025. Globally, other nations are also advancing programmable money initiatives. The Bank of Thailand has introduced an enhanced regulatory sandbox, focusing first on programmable payments. This lets financial institutions and fintech companies test automated transactions under regulatory oversight. In the private sector, the Digital Cash SDK 2.6 incorporates programmable money features like targeted subsidies, real-time settlements, and compliance automation. This builds on existing systems such as India's direct benefit transfer program, which could use programmable money to ensure subsidies—like food or fuel assistance—are spent only on designated goods or services.

WHY IT MATTERS

Programmable money could transform the industry by reducing reliance on traditional banking systems while enhancing speed, transparency, and security. Automated payments governed by smart contracts ensure transactions occur only when conditions are met. Governments and businesses can use this for conditional payments like rent, triggered by salary deposits, to ultimately cut errors and delays while boosting efficiency.

This technology could also improve cross-border payments. Programmable money enables instant settlements, benefiting global commerce and remittances. Central banks experimenting with CBDCs could link digital currencies internationally to send money across borders seamlessly.

Programmable money would also advance regulatory compliance and fraud prevention. government assistance funds could be programmed to ensure intended use, while automated anti-money laundering checks enhance trust in digital systems. For businesses, including solo entrepreneurs, programmable money unlocks new models like dynamic pricing based on demand or inventory levels and viable microtransactions due to lower costs.

In decentralized finance (DeFi), programmable money could spur innovation by enabling tokenized assets and new investment mechanisms. Real-world assets like real estate could be tokenized for easier transfers across borders. Financial institutions must adapt as smart contracts increasingly handle loans and payments with minimal human intervention.

4TH YEAR ON THE LIST

FRICTIONLESS PAYMENTS

WHAT IT IS

Frictionless payments remove obstacles in the checkout process, making transactions seamless and nearly invisible. From biometric authentication to embedded payments, these innovations enhance security and improve customer experience.

HOW IT WORKS

Frictionless payments eliminate manual steps, reduce wait times, and create seamless transactions. These payments rely on advanced authentication, automation, and data-driven personalization to function in the background.

Some of these systems rely on biometrics, authenticating users through physical characteristics such as fingerprints and facial recognition. Amazon One enables customers to pay by scanning their palm, linking the biometric data to a stored payment method. J.P. Morgan Payments piloted biometric authentication at the Miami Grand Prix, where it processed transactions in under a second, demonstrating how this technology can streamline high-traffic events.

Other systems use embedded payments; these integrate payment processing directly into an application or service, so customers can make purchases without a separate checkout step. Uber pioneered this model, where riders complete transactions effortlessly without pulling out a card or cash. Skipify and Synchrony recently introduced an embedded payment system that autofills payment details, recognizes cardholders, and enables instant access to rewards. US Bank provides merchants with embedded payment software, making the purchasing process frictionless.

AI-driven fraud detection, tokenization, and biometric security measures ensure these payments remain secure. As frictionless payments become more widespread, financial institutions and retailers must balance convenience with privacy and cybersecurity.

WHY IT MATTERS

Frictionless payments are reshaping customer expectations, leading consumers to increasingly demand effortless transactions. Traditional banks face mounting pressure from fintechs and tech giants offering mobile wallets, contactless payments, and embedded finance. Businesses failing to deliver seamless payment experiences risk losing loyalty in competitive markets, where speed and ease are key differentiators.

But the benefits of frictionless payments go beyond retaining customers: They also generate valuable data to inform risk assessments, personalize offerings, and enhance marketing. For example, insurers can use payment data to refine underwriting or develop tailored policies. These innovations boost efficiency by automating recurring transactions like loan repayments or insurance premiums, reducing costs and errors. Instant digital payouts for claims or loans improve cash flow and customer satisfaction.

Security is critical, and many frictionless payments integrate advanced methods like biometrics and AI-driven fraud detection to mitigate risks while maintaining seamless experiences. Real-time, cross-border transactions further disrupt traditional models, with open banking enabling faster transfers at lower costs. An institution adopting frictionless payments signals innovation and security, building trust, optimizing operations, and positioning the company for growth in an evolving financial landscape.

4TH YEAR ON THE LIST

INSTANT PAYMENTS

WHAT IT IS

Instant payments are becoming a regulatory requirement and competitive necessity worldwide. While adoption grows, challenges around legacy infrastructure, interoperability, and compliance remain. The next five years will define winners and laggards in real-time payments.

HOW IT WORKS

Instant payments allow funds to be transferred between accounts in real time, making them available immediately, 24/7. Unlike traditional bank transfers, which can take hours or even days to clear, instant payments are processed within seconds. These transactions typically rely on real-time payment rails—such as the EU's SEPA Instant Credit Transfer, the US's FedNow and RTP networks, or Brazil's Pix. However, interoperability challenges persist, with no standardized verification system.

In Europe, the Instant Payments Regulation (IPR) mandates that by 2025, all EU payment service providers (PSPs) must be able to send and receive instant payments, with staggered deadlines for non-EU and nonbank PSPs through 2027. Compliance requires banks to process transactions at scale, verify payee details, and conduct real-time sanction screening. In the US, there's a rapid growth in demand for instant payments, with the amount of money transferred this way expected to surpass $58 trillion by 2028. Yet, adoption is slow—only a fraction of US banks are onboard with RTP or FedNow, and less than 1% use both. Other global markets offer valuable lessons. Brazil's Pix, launched in 2020, now processes more than 36 billion transactions annually, demonstrating the potential for mass adoption. Canada's Real-Time Rail (RTR) system is set to launch by 2026, positioning the country to learn from earlier adopters and implement a modernized, scalable solution.

WHY IT MATTERS

As real-time payments become the norm, businesses and banks will need to adapt to faster transaction speeds, new compliance requirements, and shifting revenue models. For banks, this is both an opportunity and a challenge. On one hand, instant payments provide a competitive edge, reducing settlement risks and improving customer satisfaction. On the other, legacy infrastructure, processing speed limitations, and regulatory compliance create significant barriers. Of the banks currently capable of instant payments, only 10% can process more than 300 transactions per second. This may not be enough once corporations start using instant payments for mass disbursements like payroll and pensions.

Regulation is pushing banks to accelerate adoption. The EU's IPR mandates instant payments, forcing PSPs to enhance their systems despite interoperability concerns. Meanwhile, in the US, growing demand could eventually pressure more banks to join RTP or FedNow. However, there is a long road ahead: Out of more than 4,500 institutions, only 570 banks are on RTP and 700 are on FedNow.

Fintechs and digital banks have a major opportunity to gain market share. Without the constraints of legacy systems, they can move faster than traditional banks in offering seamless instant payment solutions. The rapid adoption of Pix in Brazil and the forthcoming RTR in Canada suggest that instant payments will soon be the global standard. Those that fail to adapt will risk losing customers and relevance in the financial ecosystem.

The shift towards instant and faster payments has been gathering pace... I believe that 2024 will be the year when instant payments... truly enter the mainstream consciousness across Europe.

Lena Hackelöer, CEO & Founder of Brite Payments

3RD YEAR ON THE LIST

DIGITAL WALLETS

WHAT IT IS

Digital wallets are evolving beyond payments, integrating identity verification, biometric authentication, and flexible spending options. Innovations from Visa, Apple, and the EU are expanding digital wallet functionality, making them central to personal finance.

HOW IT WORKS

Over the past year, digital wallets have advanced beyond simple payment tools to multifunctional platforms. Visa's Flexible Credential gives users control over their transactions, allowing them to switch between debit; credit; Buy Now, Pay Later (BNPL); or rewards points within a single card. Meanwhile, its Tap to Everything is expanding NFC-based interactions, enabling seamless peer-to-peer payments, secure authentication, and faster onboarding of new cards.

Security and fraud prevention are also becoming more sophisticated. The Visa Payment Passkey Service, built on Fast Identity Online (FIDO) standards, replaces passwords and one-time codes with biometric authentication for a more secure and frictionless payment experience. Apple's iOS 18 Wallet update introduces new Apple Pay features, including reward redemption, installment payments, and Tap to Cash, which enables instant money transfers between iPhones. Additionally, Apple Wallet is expanding digital ID support across multiple US states.

On a broader scale, governments are integrating digital wallets into public infrastructure. The European Digital Identity Wallet, now in development, will hold a variety of personal documents—including payment methods, travel credentials, and medical records—allowing EU citizens to securely store and share their verified identity across the bloc.

WHY IT MATTERS

As digital wallets integrate more functions, they are becoming the de facto financial hub for consumers, offering unparalleled convenience. This shift has significant implications for financial service providers. Banks and payment processors must adapt to consumer demand for seamless, multi-modal transactions, as evidenced by Visa's Flexible Credential. BNPL services, loyalty programs, and even traditional credit models may need to adjust their offerings to remain competitive within digital wallets.

Security concerns are paramount, and the rapid adoption of digital IDs and biometric authentication creates new vulnerabilities. A single compromised wallet could expose financial, medical, and personal identity data at once. Financial institutions will need to balance enhanced security measures with ease of use, ensuring consumers trust these new systems. Additionally, as governments and private companies take different approaches to digital identity, interoperability will become critical—particularly in cross-border transactions and regulatory compliance.

As digital wallets continue to expand, the question is no longer whether they will replace physical wallets but rather how deeply they will integrate into everyday life. Financial services providers must prepare for a future where digital wallets serve as both a financial tool and a primary identity credential.

SCENARIO YEAR 2029

THE 10-SECOND PAYCHECK

By 2029, the widespread adoption of instant payment systems like FedNow and RTP has transformed payroll processing in the US, enabling 90% of salaries to land in workers' accounts within seconds of completing a shift. Gig economy platforms such as Uber and DoorDash leverage this infrastructure to disburse earnings immediately after drivers or delivery personnel finish tasks, eliminating the traditional 1–3 day payment delays. This shift is further enhanced by programmable money frameworks, inspired by India's e-rupee model, which give employees a choice of embedding rules directly into digital currencies—for example, they can automatically divert 30% of earnings to rent payments when their daily income exceeds $500. Digital wallets like Apple's Tap to Cash and Visa's Flexible Credential enable workers to split funds instantly across savings, debit, or BNPL accounts, while AI-driven compliance systems (similar to J.P. Morgan's biometric authentication) screen transactions in real time to prevent fraud.

Legacy banks face existential threats as fintechs offering "smart accounts" with automated budgeting tools capture market share, while payday lenders collapse under reduced demand for cash advances. The IRS capitalizes on blockchain-based transparency to increase audits by 40%, scrutinizing previously opaque gig economy income streams. Though financial stress drops 35% due to instant liquidity access, critics highlight algorithmic biases in programmable rules—lower-income users face disproportionate compliance flags, sparking debates about fairness in automated financial systems. Policymakers respond by proposing universal basic income pilots built on FedNow's infrastructure, testing how real-time disbursements could reshape social safety nets. Meanwhile, the EU's Instant Payments Regulation pressures global banks to adopt similar systems, creating a ripple effect that accelerates real-time payroll adoption in markets like Brazil and Canada.

GOVERNANCE

12TH YEAR ON THE LIST

ALTERNATIVE CREDIT SCORING

WHAT IT IS

AI–driven alternative credit scoring models analyze nontraditional data to assess creditworthiness, improving financial inclusion. While these models enhance accuracy and fairness, there are still concerns about bias, privacy, and regulatory compliance. Standardization and transparency will be critical.

HOW IT WORKS

Traditional credit scoring relies on a limited set of financial data—mainly credit history, outstanding debt, and repayment behavior. Alternative credit scoring expands this approach, leveraging AI and machine learning to take diverse data sources into account, including rent and utility payments, bank transactions, employment history, social media activity, and online behavior.

Machine learning algorithms identify patterns in this data to predict a borrower's credit risk more precisely. Companies like Tala and Upstart analyze smartphone usage, transaction history, and employment records to score applicants who lack conventional credit histories. Hybrid models, such as those used by Zest AI and Kabbage, merge traditional scores with real-time financial data to improve accuracy. VantageScore's latest model integrates open banking data, offering a 10% predictive boost over previous versions.

These systems, while powerful, introduce complexity. AI models consider thousands of variables, making their decision-making processes difficult to interpret. Regulators and industry leaders must balance innovation with accountability, to ensure fair and transparent lending practices.

WHY IT MATTERS

Alternative credit scoring has the potential to expand financial access for millions who are underserved by traditional credit models. People without established credit histories—gig workers, recent immigrants, and younger consumers—can demonstrate creditworthiness through alternative data, potentially reducing systemic inequalities in lending.

However, the shift to AI-driven risk assessments raises serious concerns. Data privacy is a major issue, as these models require access to sensitive personal information. The use of nontraditional data also introduces new risks of bias—some behavioral indicators could disproportionately disadvantage specific demographics. Regulatory oversight remains fragmented, with existing consumer protection laws struggling to keep pace with AI-powered lending decisions. Transparency is another challenge. Consumers may not understand what factors influence their credit scores, making it difficult to dispute inaccuracies. Without industry-wide standardization, different lenders could arrive at vastly different credit decisions for the same applicant.

Financial institutions adopting alternative credit scoring must navigate regulatory complexities, integrate new data sources, and ensure their models are fair and explainable. While AI offers unprecedented insights into creditworthiness, responsible implementation will determine whether these innovations truly improve financial equity or reinforce existing barriers.

5TH YEAR ON THE LIST

RISING CYBER RISK

WHAT IT IS

Financial institutions face an unprecedented surge in cyberthreats, with attacks increasing by 75% in Q3 2024 compared to 2023. This trend is reshaping the industry's approach to cybersecurity, driving innovation in risk management and insurance strategies.

HOW IT WORKS

Increasing cyber risk has far-reaching implications for financial institutions. It's expensive, with the global average cost of a data breach reaching $4.88 million in 2024. According to the International Monetary Fund, the potential impact of extreme losses has risen as well, with an estimate that a cyber incident is expected to result in a $2.5 billion loss once every 10 years.

These cyber incidents can manifest through various channels and attack vectors. Ransomware remains a dominant threat, with sophisticated groups like BlackCat (ALPHV) causing significant disruptions, such as the February 2024 attack on Change Healthcare. Payment diversion fraud has emerged as a potent threat, affecting 58% of organizations in 2024, up from 34% the previous year. Cybercriminals are leveraging AI to create more sophisticated phishing attacks and automate hacking processes, adding a new dimension to the threat landscape.

The interconnectedness of digital systems has also introduced systemic vulnerabilities, such as the widespread disruptions caused by the CrowdStrike-Microsoft outage in July 2024. Despite these incidents, the cyber insurance landscape is evolving, with premium rates decreasing by 17% in 2023, though insurers are adjusting strategies and adding restrictions. Regulatory focus has intensified, with the US government working to quantify cyberattack impacts on critical infrastructure, including financial markets, potentially leading to new compliance requirements.

WHY IT MATTERS

Operational resilience has become paramount, as cyber incidents can lead to significant disruptions, necessitating robust risk management strategies and incident response plans. Increased regulatory scrutiny may result in new compliance requirements, potentially including federal insurance responses, impacting operational costs and risk management practices. The evolving cyber insurance market requires financial institutions to reassess their coverage and risk transfer strategies, potentially leading to increased self-insurance or alternative risk management approaches.

To combat sophisticated threats, companies will need to invest in advanced technologies like AI and machine learning for enhanced cybersecurity. Recent incidents have highlighted the need for robust vendor risk management and supply chain security, expanding the scope of cybersecurity efforts beyond internal systems. The cybersecurity talent shortage remains a critical challenge, with 26% of business leaders admitting to insufficient resources for managing cyber threats. Moreover, cyber incidents can significantly damage a financial institution's reputation, potentially leading to loss of customer trust and business opportunities.

As the digital financial ecosystem continues to expand, financial institutions must proactively adapt, balancing innovation with security, and developing agile risk management strategies to protect their assets, customers, and reputation.

3RD YEAR ON THE LIST

DATA MINIMIZATION

WHAT IT IS

States are increasingly stepping up to implement stringent data minimization standards. However, their efforts face significant resistance from powerful lobbying groups, making the passage of effective legislation a complex and contentious process.

HOW IT WORKS

Data minimization refers to the practice of limiting the collection and processing of personal data to only what is necessary for specific, clearly defined purposes. This concept is increasingly a cornerstone of state-level privacy regulations in the US as federal legislation lags in providing comprehensive data protection.

In a significant move, the California Privacy Protection Agency issued its first enforcement advisory, emphasizing the importance of data minimization under the California Consumer Privacy Act. Vermont's new data privacy law, passed in May 2024, is another example of a state-level initiative aimed at enforcing data minimization. It's notable for allowing individuals to sue companies for violating their privacy rights, a provision that sets a new standard in privacy protection and adds a significant enforcement mechanism to data minimization efforts. In Maine, lawmakers rejected two competing data privacy bills; both were the subject of intense tech industry lobbying, and underscore the challenges that state lawmakers face when trying to implement robust data protection measures.

At the federal level, the Federal Trade Commission is exploring new regulations to address the growing concerns around commercial surveillance and data security. This initiative aims to curb businesses' excessive collection and use of personal data, reflecting a broader shift toward recognizing the risks associated with data hoarding practices.

WHY IT MATTERS

The increasing focus on data minimization reflects a growing recognition of the risks associated with excessive data collection. As businesses gather vast amounts of personal information, the potential for misuse, data breaches, and privacy violations escalates. State-level actions on data minimization are critical because they set precedents that could influence broader national standards. With federal legislation still lacking, states are becoming the testing grounds for data protection strategies that could eventually shape nationwide policies.

The resistance from powerful lobbying groups indicates the high stakes. The outcomes of these legislative battles will determine the future of data privacy in the US and the balance of power between public interests and corporate influence. As more states push forward with their own data minimization laws, we could see a patchwork of regulations that vary significantly across the country, creating challenges for businesses operating in multiple jurisdictions.

In the long run, the trend toward data minimization could lead to a paradigm shift in how personal data is handled, moving away from the current model of data hoarding to one that prioritizes privacy and security. This shift could drive innovation in data processing technologies, encourage the development of new business models that do not rely on extensive data collection, and ultimately lead to a more privacy-conscious digital landscape.

1ST YEAR ON THE LIST

AI LIABILITY

WHAT IT IS

The increasing use of AI in decision-making processes is generating liability risks for businesses, particularly in sectors like health care and finance, creating new legal, financial, and reputational risks.

HOW IT WORKS

As AI systems take on more decision-making roles, the potential for liability grows. AI liability refers to the legal responsibility that companies might face when their AI systems cause harm or make decisions that are later deemed biased or incorrect. This issue is particularly acute in sectors where decisions have significant impacts on people's lives, such as health care and finance.

In one example, AI is being used by Medicare Advantage insurers to decide when to cut off care. These decisions, often made by algorithms like those created by NaviHealth, can result in premature denial of necessary care, impacting seniors who rely on these benefits. The algorithms can prioritize cost-efficiency over patient care, leading to appeals and disputes when care is denied without fully considering individual patient needs. In the financial sector, banks and insurers use AI for everything from underwriting to fraud detection. However, the risks associated with AI errors are significant. For instance, an AI model that makes a wrong trading decision or an underwriting algorithm that discriminates against certain demographics could lead to substantial financial losses and legal challenges. In a recent case, a federal judge allowed a lawsuit against Workday's AI screening software, which allegedly discriminated against job applicants based on race, age, and disability, to proceed. This highlights the growing scrutiny of AI tools in hiring and the potential for legal challenges when AI-driven decisions are perceived as biased.

WHY IT MATTERS

The complexity of AI systems makes error identification and rectification challenging, increasing liability. As AI becomes integral to business operations, comprehensive governance frameworks and accountability mechanisms are crucial. However, a survey found only 16% of health care organizations have system-wide AI governance policies, highlighting the gap between adoption and risk management.

Similarly, as AI integrates deeper into financial operations, regulatory scrutiny intensifies. Financial institutions must ensure AI systems comply with evolving standards, requiring investments in compliance, auditing, and robust governance frameworks. Many firms are unprepared, risking regulatory penalties and erosion of customer trust if AI decisions are perceived as unfair.

Despite risks, AI's prevalence in financial services presents a market opportunity: AI liability insurance. As companies recognize potential AI-related errors and financial fallout, demand for specialized insurance could surge, and insurers developing tailored AI risk policies could capture a lucrative market segment. This opportunity extends to innovative products addressing unique AI challenges, such as automated decision-making errors or AI misuse in critical financial processes.

SCENARIO YEAR 2026

FINANCEEATER

The Cyber Pandemic of 2026 began with a sophisticated ransomware attack on a major US health care provider in March, exploiting a previously unknown vulnerability in widely used financial software. The malware, dubbed “FinanceEater,” was designed to specifically target interconnected financial systems. Its rapid spread was facilitated by several key factors, including a zero-day exploit in popular financial transaction processing software, AI-powered adaptation that made it difficult for traditional antivirus systems to detect, and a supply chain attack that infected multiple organizations simultaneously through software updates.

FinanceEater’s ability to hop from one system to another was particularly devastating. It exploited APIs used for interbank communications, allowing it to spread across different financial institutions rapidly. Once inside a system, the malware stole authentication credentials to access connected systems and partner networks. It also compromised shared cloud services used by multiple financial entities, creating a web of infection across seemingly isolated systems. Additionally, FinanceEater specifically targeted high-frequency trading platforms, using their lightning-fast connections to propagate across global stock exchanges within minutes.

As the attack flourished, it paralyzed electronic trading systems, froze millions of bank accounts, and compromised sensitive financial data of countless individuals and businesses. By June 2026, more than 70% of major financial institutions worldwide had reported significant operational disruptions, leading to a temporary shutdown of stock exchanges and a global economic crisis. The cyber pandemic was finally contained in September 2026 through an unprecedented international collaboration of cybersecurity experts, government agencies, and tech giants. This collaborative effort led to the development of an AI-powered defense system capable of predicting and neutralizing FinanceEater’s evolving attack vectors in real time, finally bringing the global financial crisis under control.

INSURANCE

The use of artificial intelligence by the insurance industry could make some people ‘uninsurable’… We want safe and responsible use of AI to drive beneficial innovation, but also an open conversation about the risks and trade-offs.

Nikhil Rathi, Chief Executive of the UK’s Financial Conduct Authority

1ST YEAR ON THE LIST

AI IN UNDERWRITING

WHAT IT IS

AI is revolutionizing underwriting through augmented and algorithmic approaches, blending human expertise with automated decision-making. While it enhances efficiency, the technology's infancy introduces challenges, requiring careful adoption and regulation.

HOW IT WORKS

In underwriting, AI is generally used in one of two ways: augmented underwriting, where AI processes the data but human underwriters apply their judgment to complex cases, or algorithmic underwriting, where AI analyzes data, assesses risks, and issues policy decisions.

State Farm has led the industry in AI-related patent filings. One is for a system that utilizes real-time vehicle data—driving behavior, vehicle conditions, and location-based risks—to generate dynamic insurance quotes. Another patent uses generative adversarial networks to fill gaps in 3D data, which could significantly improve the accuracy of damage assessments and claims processing.

As highlighted by the New York Department of Financial Services' AI Circular Letter, regulators are increasingly focused on ensuring AI underwriting models are transparent, nondiscriminatory, and actuarially sound. As of the end of 2024, the NAIC bulletin on AI use for insurers had been adopted by 21 states. (See map on next page.)

This shift toward AI-driven underwriting is not without its challenges. Underwriting has traditionally relied on deep, experiential knowledge, especially in specialized lines of insurance where subtle risk factors play a crucial role. In their current form, AI systems may not yet fully capture these complexities, potentially overlooking nuances experienced underwriters would consider.

WHY IT MATTERS

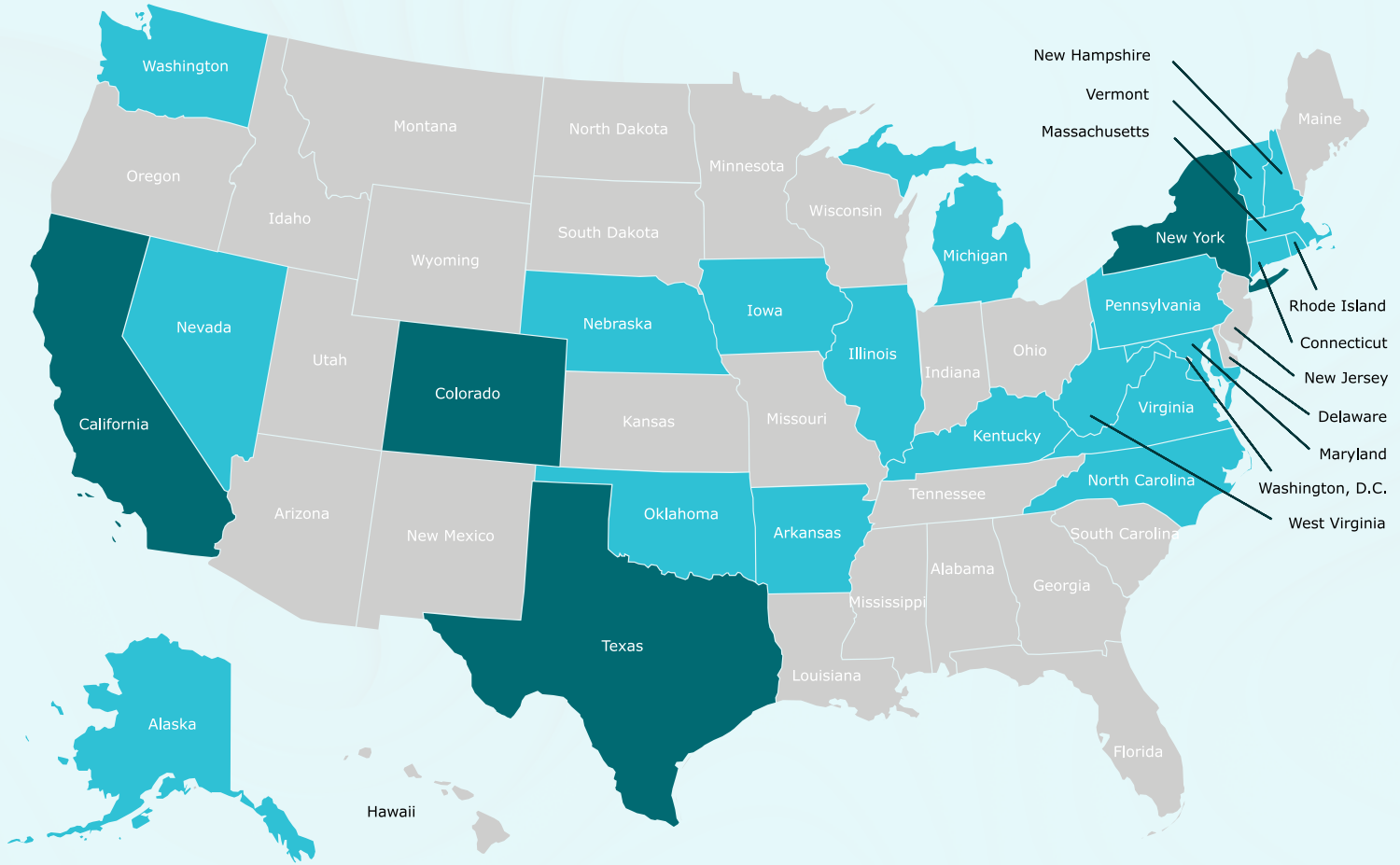
AI-driven processes can drastically reduce the time needed to assess risks and issue policies, improving customer satisfaction and enabling insurers to handle higher volumes of applications more efficiently. However, this also introduces heightened regulatory scrutiny. Compliance with evolving standards, such as those outlined by the NYDFS, will require insurers to invest in governance frameworks that ensure AI models are transparent, fair, and free from bias. Failure to meet these standards could lead to legal challenges, fines, and reputational damage.

The shift to AI-driven underwriting will also impact workforce dynamics. Traditional underwriting roles may evolve, requiring underwriters to develop new skills to work effectively with AI tools. Companies may need to invest in training programs to bridge the gap between traditional and data-centric skills. As more routine tasks are automated, the demand for entry-level underwriting positions may decline while the need for data scientists and AI specialists within insurance companies increases.

Competitive advantage in the insurance industry will increasingly depend on the successful integration of AI. Companies that can harness AI to offer more personalized, efficient services will gain an edge in a market that values speed and accuracy. However, this advantage comes with managing the risks associated with AI, including ensuring compliance with regulations and addressing potential biases within AI models.

Implementation of NAIC Model Bulletin: Use of Artificial Intelligence Systems by Insurers

Status as of February 1, 2025



- **Adopted** (21-Jurisdictions)
- **Insurance Specific Regulation/Guidance** (4-Jurisdictions)

Source: NAIC

1ST YEAR ON THE LIST

PARAMETRIC INSURANCE

WHAT IT IS

Parametric insurance, with its automatic payouts based on preestablished triggers, is positioned to transform risk management as advancements in sensor technology and climate volatility heighten the need for rapid, data-driven solutions.

HOW IT WORKS

Unlike traditional indemnity-based insurance that assesses actual damage post-event, parametric insurance relies on predefined triggers, such as specific weather conditions or seismic activities, to automatically activate payouts. For example, a parametric policy covering hurricane damage might stipulate that if a hurricane of Category 4 or higher passes within a 50-mile radius of the insured location, the company will issue a payout. The critical aspect here is the reliance on external, third-party data sources—such as meteorological agencies or Internet of Things–based sensors—that confirm the occurrence and intensity of the triggering event.

The technology behind parametric insurance has evolved significantly. Companies like Safehub are at the forefront, utilizing sophisticated sensors capable of capturing building-specific data such as Peak Ground Acceleration during an earthquake. These sensors provide granular data that goes beyond general regional measurements; this ensures that the response is tailored to the specific impact on the insured property, reducing the potential for disputes.

Increasingly, parametric insurance models are incorporating machine learning and predictive analytics—as well as historical data—to refine the accuracy of trigger definitions. This is particularly crucial as climate change continues to alter traditional risk models, making historical data less reliable for predicting future events.

WHY IT MATTERS

The growing unpredictability of natural disasters, driven by climate change, is rendering traditional insurance models less effective. These models are often slow, which can delay critical financial support. Parametric insurance addresses these shortcomings by offering near-instant payouts based on clear, predefined criteria, providing essential liquidity in the immediate aftermath of a disaster. Its ability to provide quick financial relief is especially vital for vulnerable sectors like agriculture: In one example, a farmer in the Philippines with a parametric policy was able to receive a payout immediately after a flooding event, enabling him to replant crops without delay. This outcome would have been impossible under a traditional policy.

As sensor technology continues to advance, the precision and reliability of parametric triggers will improve. The use of site-specific data from sensors like those deployed by Safehub not only enhances the accuracy of risk assessments but also opens up new possibilities for customizing insurance products to meet the unique needs of individual properties or businesses.

But widespread adoption of parametric insurance still faces challenges, primarily due to a lack of understanding among potential customers about how these products work. Insurers must invest in education and transparency—as well as ensure the robustness and reliability of the technologies underpinning parametric insurance to maintain trust and efficacy.

1ST YEAR ON THE LIST

CLIMATE IMPACT ON INSURERS

WHAT IT IS

Climate-related disasters are forcing insurers to adopt advanced predictive models and rethink risk management. Rising premiums and market exits are increasing as insurers grapple with unpredictable weather patterns and rising claims from natural disasters.

HOW IT WORKS

Severe weather is accelerating an insurance crisis. In 2024, natural catastrophes (nat cats) accounted for an estimated $320 billion in losses worldwide, but only slightly more than half of that was insured. Historically, hurricanes and earthquakes make up for a majority of those losses, but wildfires are giving other nat cats a run for their money. Experts currently estimate that losses resulting from the January Los Angeles wildfires alone will exceed $250 billion. For years, insurers have been raising premiums or exiting altogether; several insurers had halted new home insurance policies in California even before the recent wildfire blitz. The trend extends beyond California; insurers are also withdrawing from Colorado, Florida, and Louisiana. As private insurers retreat, state-backed “last-resort” plans are under pressure. The California FAIR Plan now carries $458 billion in property exposure—an increase of 61% from the previous year.

To counter these risks, insurers have adopted AI-driven climate modeling. Munich Re and Swiss Re are integrating real-time wildfire prediction models, using satellite imagery, drought indices, and wind pattern analysis to forecast wildfire spread. Allstate has expanded its machine-learning risk assessment system to better predict property damage from simultaneous climate events, such as windstorms combined with wildfires. Regulatory changes are also underway—California’s insurance commissioner is considering allowing insurers to factor long-term climate projections into their pricing models.

WHY IT MATTERS

Climate-driven loss frequency and severity will continue to increase over the next decade or two, both in the “usual suspect” regions and in less expected geographic areas, such as regions of the Northeast due to flooding and wind damage. In particular, flooding outside traditional floodplains is expected to increase property losses by 40%–50% over the next 20 years. These losses are driven by some non-climate specific factors as well—namely demographic growth in key geographic regions, and the impact of inflation on construction costs—but the losses that do occur stem from climate-specific events, which will continue to intensify.

The approach for property and casualty insurers has been to withdraw from high-risk markets. However, insurers will need to develop more sophisticated solutions to address the challenge in order to maintain their market penetration. Health insurers will also feel the effects. Research shows that extreme weather events, like heat waves and wildfires, are leading to a rise in hospitalizations. As these weather events become more common, health insurers will need to reassess their risk models, premiums, and coverage options.

The increase in climate-related events and losses over the last several years sets the stage for the new normal. Insurers in all sectors have survived up to now, but to succeed in the future, they’ll need to find new ways to thrive.

1ST YEAR ON THE LIST

FRAUD MITIGATION

WHAT IT IS

Fraud mitigation in insurance is evolving rapidly, with AI and machine learning at the forefront. New solutions leverage advanced analytics, behavioral data, and real-time processing to detect complex fraud patterns, reduce false positives, and enhance operational efficiency for insurers.

HOW IT WORKS

Insurers are increasingly adopting AI-powered fraud detection technologies to improve accuracy, reduce losses, and enhance customer experiences. RSA Insurance's partnership with Clearspeed exemplifies this trend: Clearspeed's technology uses AI-powered voice analytics to assess claim legitimacy and rapidly flag high-risk cases, allowing RSA to focus investigative efforts where needed while expediting low-risk claims.

Other industry leaders are also investing in AI-driven fraud detection. SAS Institute introduced an AI-powered solution that uses machine learning to reduce false positives, while FICO upgraded its fraud detection platform with advanced AI analytics to uncover complex fraud patterns. In Brazil, Solutis partnered with FICO to offer AI-powered risk assessment tools for midsize banks and insurers, improving fraud prevention and customer personalization.

New AI solutions also integrate behavioral data analytics. ForMotiv and FRISS joined forces to analyze thousands of digital behavioral data points during the application process, so insurers can detect inconsistencies and potential fraud in real time. Meanwhile, the Insurance Fraud Bureau (IFB) and Shift Technology launched IFB Exploration in the UK, leveraging AI analytics to detect organized fraud networks across insurers.

WHY IT MATTERS

Fraud costs the insurance industry billions annually, with opportunistic fraud and organized crime networks creating significant financial strain. AI-driven fraud detection is crucial for reducing these losses, increasing efficiency, and maintaining consumer trust. By leveraging AI, insurers can automate fraud detection processes to reduce human error and accelerate decision-making.

Beyond cost savings, AI-powered fraud detection also improves customer experiences. Faster claims processing for low-risk cases ensures that legitimate customers receive payouts more quickly, while fraudsters are identified with greater precision. The competitive landscape is evolving as insurers integrate AI into risk assessment strategies. Companies that fail to adopt AI-based fraud detection risk falling behind under higher losses and operational inefficiencies. Meanwhile, regulatory bodies and industry organizations are monitoring AI's role in fraud prevention, ensuring ethical considerations and bias mitigation remain priorities.

As AI fraud detection systems grow more sophisticated, the industry must balance automation with transparency. Understanding how AI models make decisions will be crucial for regulatory compliance and customer trust. Looking ahead, expect insurers to refine fraud detection models with even more granular data inputs that will lead to highly personalized and adaptive fraud prevention strategies.

1ST YEAR ON THE LIST

CLAIM ENHANCEMENTS

WHAT IT IS

Property and casualty (P&C) insurers are leveraging artificial intelligence to automate and accelerate claims processing. AI–powered underwriting, fraud detection, and real–time damage assessments are reducing costs and improving the customer experience.

HOW IT WORKS

AI-driven claims processing is transforming P&C insurance by automating key functions in underwriting, fraud detection, and claims estimation. Insurers such as Travelers, Zurich, CCC Intelligent Solutions, Clearcover, and Snapsheet are deploying AI models trained on years of claims data to enhance decision-making and improve efficiency.

At Travelers, the company has developed an AI large language model, trained specifically on Travelers documents and decisions, that ingests documents and analyzes lawsuit documents. Zurich is feeding six years of claims data into generative AI models to identify risk patterns, refine policy pricing, and reduce loss ratios.

AI is also reducing processing times by automating damage assessment and fraud detection. CCC Intelligent Solutions and Clearcover use AI-powered image recognition to assess accident damage from user-submitted photos, allowing insurers to provide near-instantaneous damage estimates. This eliminates the need for adjusters to manually inspect vehicles, cutting processing times from weeks to hours. Snapsheet extends AI-driven automation further by digitizing the full claims process, including fraud detection. By integrating AI with cloud-based claims management systems, Snapsheet's tools can identify false claims and process legitimate ones faster. These solutions, powered by computer vision, natural language processing, and predictive analytics, enable insurers to handle higher claim volumes with fewer resources.

WHY IT MATTERS

AI-driven claims processing requires significant investment in data infrastructure, machine learning models, and cloud-based automation. Insurers must integrate AI with legacy systems, train models on diverse claims data, and ensure regulatory compliance. Despite these costs, the long-term benefits are substantial. AI can reduce claims processing expenses by up to 30%, improve fraud detection accuracy, and accelerate settlements—leading to higher customer satisfaction and lower operational costs.

For carriers, measurable improvements include faster cycle times, reduced loss adjustment expenses, and enhanced underwriting precision. AI-powered claims automation enables insurers to process higher volumes without increasing headcount, improving scalability and profitability. Fraud detection algorithms help carriers mitigate billions in losses, strengthening overall financial performance.

Challenges remain. AI models must be continuously refined to prevent bias and maintain accuracy. Insurers must also navigate evolving regulations on AI decision-making in claims. Additionally, as claims processes become more digitized, cybersecurity threats targeting sensitive policyholder data will rise. To maximize AI's potential, insurers must invest not just in technology but also in governance, transparency, and security frameworks.

SCENARIO YEAR 2030

CASCADING LIABILITIES

In late 2028, a series of cyber incidents targeting logistics companies in Southeast Asia triggered a prolonged global economic challenge, exposing vulnerabilities in interconnected digital supply chains. Supply chain disruptions cascaded through industries, and business interruption and contingent business interruption claims surged, with 45% of companies reporting financial impacts from supply chain issues. The complexity of digital partnerships and blockchain-based smart contracts created scenarios of cascading liabilities that tested conventional underwriting models. Insurers struggled to adapt their policies to cover losses from unforeseen events, leading to increased litigation and reputational risks. The crisis highlighted the need for insurers to reassess risk assessment models, revise coverage terms, and develop new products to address emerging risks.

As the crisis unfolded, a clear divide emerged. Companies that had invested in advanced modeling techniques to anticipate interconnectedness in the global digital ecosystem were able to mitigate their losses. These insurers had developed sophisticated risk assessment tools that accounted for digital dependencies, allowing them to adjust their underwriting practices. In contrast, insurers who continued to rely on standard underwriting practices found themselves heavily impacted. Their traditional models failed to capture the accumulating nature of risks in the interconnected digital landscape, leaving them exposed to unexpected and substantial losses.

Now, in 2030, this disparity has reshaped the competitive landscape of the insurance industry. The crisis served as a powerful catalyst for innovation, pushing the entire sector toward more dynamic risk modeling and collaborative approaches to managing systemic vulnerabilities. The recent lessons learned have fundamentally transformed how insurance companies approach risk assessment and policy underwriting in the digital age.

AUTHORS & CONTRIBUTORS

Nick Bartlett

Financial Services and Insurance Lead

Nick Bartlett is a Director at Future Today Strategy Group and leads our Financial Services & Insurance and Transportation & Manufacturing practice areas.

Prior to FTSG, he held positions in corporate strategy and insights generation roles, serving as a partner to senior leadership at multiple Fortune 100 financial services companies. Throughout his career, he has specialized in framework design, corporate innovation, strategic management, and insurance.

Nick has an extensive background in developing strategic insights across a variety of industries (e.g., manufacturing, transportation, construction, energy) and subject matter areas (e.g., small business, mobility, robotics, platforms & ecosystems), in addition to the shifting nature of business and consumer preferences. He has deep experience in developing and implementing both trend sensing, as well as signal identification for large organizations. Nick has also led the design and establishment of internal foresight and scenario development capabilities across multiple institutions.

He serves as a coach in the strategic foresight MBA course at the NYU Stern School of Business. Nick holds both an MBA and a Bachelor of Arts in Public Relations from Quinnipiac University.

Chief Executive Officer
Amy Webb

Managing Director
Melanie Subin

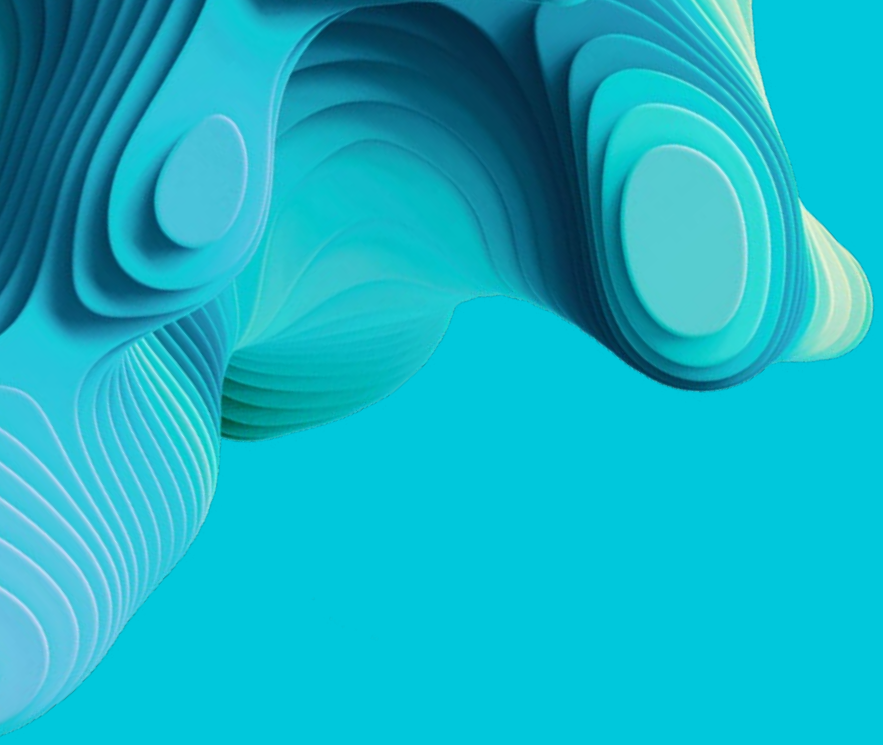
Director of Marketing & Comms.
Victoria Chaitoff

Creative Director
Emily Caufield

Editor
Erica Peterson

Copy Editor
Sarah Johnson

Melanie Subin
Managing Director,
Contributor



SELECTED SOURCES

"2024 Cryptocurrency Adoption and Sentiment Report." Security.org. https://www.security.org/digital-security/cryptocurrency-annual-consumer-report/.

Adams, David G., et al. "Treasury Department Warns Financial Institutions to Prepare for AI-Age Fraud—AI: The Washington Report." Mintz, April 4, 2024. https://www.mintz.com/insights-center/viewpoints/54731/2024-04-04-treasury-department-warns-financial-institutions.

"AXA XL Unveils New Cyber Insurance Extending Coverage to Help Businesses Manage Emerging Gen AI Risks." AXA XL, October 21, 2024. https://axaxl.com/press-releases/axa-xl-unveils-new-cyber-insurance-extending-coverage-to-help-businesses-manage-emerging-gen-ai-risks.

Braun, Helene. "Investment Giant Vanguard Blocks Clients From Buying Bitcoin ETFs." CoinDesk, January 11, 2024. https://www.coindesk.com/business/2024/01/11/investment-giant-vanguard-blocks-clients-from-buying-bitcoin-etfs/.

"California Privacy Protection Agency Issues First-Ever Enforcement Advisory." WilmerHale, April 10, 2024. https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240410-california-privacy-protection-agency-issues-first-ever-enforcement-advisory.

"CFPB Launches Process to Recognize Open Banking Standards." Consumer Financial Protection Bureau, June 5, 2024, https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-process-to-recognize-open-banking-standards/.

"CN114202908 Vehicle Early Warning Method, Device, and Equipment Based on Disaster Weather and Storage Medium." https://patentscope.wipo.int/search/en/detail.jsf?docId=CN356052549&_cid=P22-M0NV9K-74187-8.

"CN114236643 Weather Forecasting System-Based Weather Forecasting Method, Device, Equipment and Medium." https://patentscope.wipo.int/search/en/detail.jsf?docId=CN357092161&_cid=P22-M0NV9K-74187-8.

Columbus, Louis. "How Visa Is Using Generative AI to Battle Account Fraud Attacks." VentureBeat, May 7, 2024. https://venturebeat.com/security/how-visa-is-using-generative-ai-to-battle-account-fraud-attacks/.

"Commercial Surveillance and Data Security Rulemaking." Federal Trade Commission, August 5, 2022. https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

"Crunchfish Provides Programmable Money Support in Digital Cash." Cision, September 24, 2024. https://news.cision.com/crunchfish/r/crunchfish-provides-programmable-money-support-in-digital-cash,c4041615.

"Data Minimization Is the Key to a Meaningful Privacy Law." Electronic Privacy Information Center, May 9, 2024. https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/.

"Digital Wallets: Accommodating Mobile Payments & More." Ameris Bank. https://www.amerisbank.com/Personal/Learn/Financial-Articles-Advice/Managing-Your-Money/Digital-Wallets-Accommodating-Mobile-Payments-More.

"Entrust Selects Carahsoft as US Public Sector Partner for Biometrics, Digital ID." Biometric Update." August 30, 2024. https://www.biometricupdate.com/202408/entrust-selects-carahsoft-as-us-public-sector-partner-for-biometrics-digital-id.

"Exploring Spatial Heterogeneity in Synergistic Effects of Compound Climate Hazards: Extreme Heat and Wildfire Smoke on Cardiorespiratory Hospitalizations in California." Science Advances 10, issue 5 (February 2, 2024). https://www.science.org/doi/10.1126/sciadv.adj7264.

"ForMotiv and FRISS Partner to Enhance Fraud Detection and Risk Mitigation in Insurance." FRISS. https://www.friss.com/press/formotiv-and-friss-partner-to-enhance-fraud-detection-and-risk-mitigation-in-insurance.

"FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices." Federal Trade Commission, August 10, 2022. https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

GlobalData. "RSA Insurance, Clearspeed Join Hands to Improve Fraud Detection." Yahoo Finance, October 16, 2024. https://finance.yahoo.com/news/rsa-insurance-clearspeed-join-hands-162224875.html/.

Hall, Ian. "Bank of Thailand 'Enhanced' Regulatory Sandbox Focuses on Programmable Payments." Global Government Fintech, June 24, 2024. https://www.globalgovernmentfintech.com/bank-of-thailand-enhanced-regulatory-sandbox-programmable-payments/.

IBISA. "IBISA Raises $3 Million to Scale Parametric Insurance Solutions, Strengthening Climate Resilience Across Asia and Africa." June 25, 2024. https://www.prnewswire.com/in/news-releases/ibisa-raises-3-million-to-scale-parametric-insurance-solutions-strengthening-climate-resilience-across-asia-and-africa-302178042.html.

"ID in Wallet." https://learn.wallet.apple/id#states-list.

"Increasingly Popular 'Parametric Insurance' Helps Farmers and Others Hit Hard by Extreme Weather." AP News, July 12, 2024. https://apnews.com/article/extreme-weatherinsuranceclimate-changestorms-064635f482e-66a5e22dd030f3fa8b7cb.

Insights, Ledger. “Japan’s Big 3 Banks Collaborate on DLT Digital Identity Initiative.” Ledger Insights, June 20, 2024. https://www.ledgerinsights.com/japans-big-3-banks-collaborate-on-dlt-digital-identity-initiative/.

“Insurance Circular Letter No. 7 (2024): Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing.” Department of Financial Services. https://www.dfs.ny.gov/industry-guidance/circular-letters/cl2024-07.

“Insurance Fraud Detection Market to Reach USD 32.2 Billion by 2032| Driven by Rising Need for Enhanced Fraud Prevention Technologies | Research by SNS Insider.” GlobeNewswire, December 16, 2024, https://www.globenewswire.com/news-release/2024/12/16/2997579/0/en/Insurance-Fraud-Detection-Market-to-Reach-USD-32-2-Billion-by-2032-Driven-by-Rising-Need-for-Enhanced-Fraud-Prevention-Technologies-Research-by-SNS-Insider.html.

“iOS 18 Makes iPhone More Personal, Capable, and Intelligent Than Ever.” Apple Newsroom, June 10, 2024. https://www.apple.com/newsroom/2024/06/ios-18-makes-iphone-more-personal-capable-and-intelligent-than-ever/.

Jergler, Don. “Activist Report Shows More Insurers Making Climate-Related Disclosures.” Insurance Journal, June 21, 2024. https://www.insurancejournal.com/news/national/2024/06/21/780384.hftm.

Kats, Rimma. “How Biometric Payments Are Shaping the Future of Contactless Transactions.” PaymentsJournal, July 23, 2024. https://www.paymentsjournal.com/how-biometric-payments-are-shaping-the-future-of-contactless-transactions/.

“Lemonade Says AI Improved Insurance Loss Ratio.” PYMNTS.com, February 28, 2024. https://www.pymnts.com/news/artificial-intelligence/2024/lemonade-says-ai-improved-insurance-loss-ratio/.

Lunden, Ingrid. “After 6-Year Hiatus, Stripe to Start Taking Crypto Payments, Starting With USDC Stablecoin.” TechCrunch, April 25, 2024. https://techcrunch.com/2024/04/25/after-6-year-hiatus-stripe-to-start-taking-crypto-payments-starting-with-usdc-stablecoin/.

“Maryland Enacts Comprehensive Data Privacy Law.”White & Case LLP, May 14, 2024. https://www.whitecase.com/insight-alert/maryland-enacts-comprehensive-data-privacy-law.

McGee, Suzanne. “Nasdaq Seeks SEC Approval for Bitcoin Index Options.” Reuters, August 27, 2024. https://www.reuters.com/technology/nasdaq-seeks-sec-approval-bitcoin-index-options-2024-08-27/.

Mukherjee, Pradipta. “E-Rupee Set for Broader Adoption as Cloud Facility Gathers Steam.” CoinGeek, January 6, 2025. https://coingeek.com/e-rupee-set-for-broader-adoption-as-cloud-facility-gathers-steam/.

“NAIC Endorses a Model Bulletin Regarding the Utilization of AI within the Insurance Sector.” Pinnacle Actuarial Resources, June 26, 2024. https://www.pinnacleactuaries.com/article/naic-endorses-model-bulletin-regarding-utilization-ai-within-insurance-sector.

“Navigating Climate Risks: Progress and Challenges in US Insurance Sector Disclosures.” Ceres, June 18, 2024. https://www.ceres.org/resources/reports/navigating-climate-risks-progress-and-challenges-in-us-insurance-sector-disclosures.

“New Alternative Banking Data Credit Score Released.” VantageScore, May 15, 2024. https://www.vantagescore.com/press_releases/new-alternative-data-vantagescore-4plus-credit-scoring-model-boosts-predictive-power-and-financial-inclusion/.

“New Unified Fraud Technology Platform to Transform Industry’s Fight Against Fraud, Announced by IFB and Shift Technology.” Shift, January 16, 2025. https://www.shift-technology.com/resources/news/new-unified-fraud-technology-platform-to-transform-industrys-fight-against-fraud-announced-by-ifb-and-shift-technology.

“New York State Department of Financial Services Adopts AI Guidance” Mayer Brown, uly 18, 2024. https://www.mayerbrown.com/en/insights/publications/2024/07/new-york-state-department-of-financial-services-adopts-ai-guidance.

“NIST Launches Collaborative Research Effort on Digital Identity to Support Secure Delivery of Public Benefits.” NIST, June 10, 2024. https://www.nist.gov/news-events/news/2024/06/nist-launches-collaborative-research-effort-digital-identity-support-secure.

“Real-Time Rail: Instant Payments in Canada.” RedCompass Labs. https://www.redcompasslabs.com/real-time-rail-instant-payments-in-canada/.

“Rising Cyber Threats Pose Serious Concerns for Financial Stability.” IMF, April 9, 2024. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

Ross, Casey et al. “Denied by AI: How Medicare Advantage Plans Use Algorithms to Cut off Care for Seniors in Need.” STAT, March 13, 2023. https://www.statnews.com/2023/03/13/medicare-advantage-plans-denial-artificial-intelligence/.

Shumway, Emilie. “Lawsuit Alleging Workday’s AI Tools Are Discriminatory Can Move Forward, Court Says.” HR Dive, July 16, 2024. https://www.hrdive.com/news/workday-ai-tools-discrimination-lawsuit-california/721482/.

"Sigma 1/2024: Natural Catastrophes in 2023." Swiss Re, March 26, 2024. http://www.swissre.com/institute/research/sigma-research/sigma-2024-01.html.

"Skipify and Synchrony Team on Frictionless Checkouts." PYMNTS.com, March 13, 2024. https://www.pymnts.com/news/faster-payments/2024/skipify-and-synchrony-team-on-frictionless-checkouts/.

"Solutis Partners with FICO in Brazil to Offer AI-Powered Solutions to Banks and Insurers." FICO, May 1, 2024. https://www.fico.com/en/newsroom/solutis-partners-fico-brazil-offer-ai-powered-solutions-banks-and-insurers.

Team, R&I Editorial. "Businesses Report Increase in Cyberattacks in 2024." Risk & Insurance, January 16, 2025. https://riskandinsurance.com/businesses-report-increase-in-cyberattacks-in-2024/.

"The Last Mile: Financial Vulnerabilities and Risks." IMF, April 2024. https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024.

"The Many Use Cases of the EU Digital Identity Wallet - EU Digital Identity Wallet -. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+many+use+cases+of+the+EU+Digital+Identity+Wallet.

Thompsett, Louis. "Citi & Classiq: Quantum Solutions for Portfolio Optimisation." Fintech Magazine, February 9, 2024. https://fintechmagazine.com/articles/citi-explores-quantum-computing-for-portfolio-optimisation.

Thompsett, Louis. "Mastercard Launches Gen AI Tool for Consumer Protection." Fintech Magazine, February 2, 2024. https://fintechmagazine.com/articles/mastercard-launches-gen-ai-tool-to-better-protect-consumers.

"UNHCR Welcomes Commitments at ID4Africa 2024 on Digital Identity Gains for Displaced People in Africa." UNHCR, May 27, 2024. https://www.unhcr.org/news/announcements/unhcr-welcomes-commitments-id4africa-2024-digital-identity-gains-displaced.

"US11948212 Classification of Wildfire Danger." https://patentscope.wipo.int/search/en/detail.jsf?docId=US426525304&_cid=P22-M0NV9K-74187-11.

"US20240242291 Dynamic Auto Insurance Policy Quote Creation Based on Tracked User Data." https://patentscope.wipo.int/search/en/detail.jsf?docId=US435545708&_cid=P21-LZN5GC-96936-3.

"US20240242299 Regional Wildfire Vulnerability Detection." https://patentscope.wipo.int/search/en/detail.jsf?docId=US435545716&_cid=P22-M0NV9K-74187-1.

"US20240242498 Catastrophe Analysis Via Realtime Windspeed and Exposure Visualization." https://patentscope.wipo.int/search/en/detail.jsf?docId=US435545936&_cid=P22-M0NV9K-74187-1.

"Vermont Passes Data Privacy Law Allowing Consumers to Sue Companies." The Record, May 13, 2024. https://therecord.media/vermont-passes-data-privacy-law.

"Visa Extends Risk Management Solutions to Non-Visa Transactions." PYMNTS.com, March 27, 2024. https://www.pymnts.com/visa/2024/visa-reaches-outside-its-network-with-ai-to-protect-real-time-transactions/.

"Visa Reinvents the Card, Unveils New Products for Digital Age." Visa, May 15, 2024. https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20686.html.

"Why Parametric Insurance Could Be a Climate Disaster Aid Solution in the Global South." World Economic Forum, February 28, 2024. https://www.weforum.org/agenda/2024/02/why-parametric-insurance-could-be-the-solution-to-uncertain-relief-capital/.

Willard, Jack. "Munich Re's Risk Management Partners & CGI to Help Insurers Reduce Claims through Climate Risk Mitigation." Reinsurance News, July 3, 2024. https://www.reinsurancene.ws/munich-res-risk-management-partners-cgi-to-help-insurers-reduce-claims-through-climate-risk-mitigation/.

Wilson, Tom. "UK Allows Professional Investors to Use Crypto Exchange-Traded Notes." Reuters, March 11, 2024. https://www.reuters.com/technology/uk-financial-watchdog-will-not-block-requests-crypto-exchange-traded-notes-2024-03-11/.

Wright, Alex. "Next-Gen RMS: AI Brings Broader Insights and Stronger Control in Insurance Risk Management." Risk & Insurance, April 4, 2024. https://riskandinsurance.com/next-gen-rms-ai-brings-broader-insights-and-stronger-control-in-insurance-risk-management/.

Zank, Alex. "Climate Change Keeps Punching Insurers in the Wallet—2023 Was the 4th Straight Year Over $100 Billion of Natural Catastrophe Losses." Fortune, March 30, 2024. https://fortune.com/2024/03/30/climate-change-insurance-natural-catastrophe-losses-over-100-billion-2023/.

ABOUT FUTURE TODAY STRATEGY GROUP

ABOUT US

Future Today Strategy Group is a consulting firm specializing in strategic foresight, a data-driven practice for developing plausible future scenarios to inform today's decisions. As organizations across the globe grapple with an increasingly volatile and uncertain business climate, FTSG provides clarity through long-term strategic planning. Its team of subject matter experts combines best-in-class trends and technology research with actionable strategies to generate business impact. In the two decades since its founding, FTSG has become the preeminent foresight advisory to Fortune 500 companies, world governments, and other major organizations—empowering leaders to make better decisions about the future, today.

CONTACT US

For an introductory conversation to learn how FTSG can assist your organization with its strategic planning and foresight needs, please contact:

inquiries@ftsg.com

ftsg.com

+1 267 342 4300

SOCIAL

Linkedin

@Future-Today-Strategy-Group

The names of companies, services, and products mentioned in this report are not necessarily intended as endorsements by FTSG or this report's authors.

FTSG's 2025 Tech Trends Report relies on data, analysis, and modeling from a number of sources, which includes sources within public and private companies, securities filings, patents, academic research, government agencies, market research firms, conference presentations and papers, and news media stories. Additionally, this report draws from FTSG's previous reports and newsletters. FTSG's reports are occasionally updated on the FTSG website.

FTSG advises hundreds of companies and organizations, some of which are referenced in this report. FTSG does not own any equity position in any of the entities listed in this presentation.

Any trademarks or service marks used in this report are the marks of their respective owners, who do not endorse the statements in this report. All rights in marks are reserved by their respective owners. We disclaim any and all warranties, expressed or implied, with respect to this report.


FTSG