Evaluating the Role of Predictive and Generative AI in Shaping RegTech and Regulatory Practices in the FinTech Sector

Introduction

The evolution of financial technology at speed, more profound than ever before, has completely and fundamentally changed what the architecture, distribution mechanism, and regulatory oversight of financial services look like. Central to this revolution is the rise and rapid evolution of predictive and generative AI, which are fundamentally changing how financial services firms operate, compete, and comply. Specifically, **predictive AI** combines advanced machine learning models with rich and varied data sets to produce accurate predictions across a variety of use cases, including credit risk modeling, advanced fraud detection systems, and both market and behavioral prediction. By contrast, **generating AI**, as its name suggests, is perfect for producing brand-new outputs (data and insights), content generation, which then can drive the automation of complex and labor-intensive processes like regulatory report preparation and compliance documentation.

These technologies are more than an extension of existing implementation but a structural change to financial intermediation. AI promotes real-time decision-making by embedding intelligence into financial systems, improving operational efficiency, and enabling financial inclusion. Nevertheless, this ascent also brings with it some serious regulatory issues, such as data governance, algorithmic bias, cybersecurity risks, and systemic risk (Nicoletti, 2021).

At the same time as this is happening, we are also seeing growth in **RegTech** (Regulatory Technology) and **SupTech** (Supervisory Technology), a parallel transformation of regulatory approaches. The use of AI-based tools by regulators and financial institutions for compliance, monitoring, risk management, etc. Such a twin transformation of financial services and regulatory systems evokes fundamental questions about governance, stability, and the future role of regulators.

The report provides a critical assessment of how predictive and generative AI are changing financial services, evolving regulatory frameworks, and market dynamics with real-world case studies and theoretical underpinnings.

1. Analysis of Predictive and Generative AI in Financial Services

Predictive and generative AI are fundamentally transforming financial services by enhancing efficiency, reducing costs, and enabling new forms of market participation. AI and ML can be used in many types of financial activities: processing large quantities of raw data on customer behavior to find patterns, predicting outcomes (trend forecasting), automating administrative tasks and customer services, fraud detection models,

personalized “smart” services provision practices for banks; enhancement of existing modeling, quantitative finance methods that improve traditional techniques by integrating new knowledge from behavioral or casual inference; compliance activities (Nicoletti, 2021). Such a notion goes beyond deploying AI as an operational technology to being embedded in the core infrastructure of modern finance.

Predictive AI is based on historical and real-time data to predict outcomes. In terms of financial services, it is most evident in the fields of credit scoring, fraud detection, risk management, customer profiling, algorithm-based trading, and AML monitoring. For example, AI-powered credit scoring can be utilized to assess borrowers based on alternative data, such as transaction histories, utility payments, mobile money activity, employment records, and behavioral data; instead of traditional credit histories in cases where they do not exist. This may better facilitate access to credit for the underserved and the SMEs (BIS, 2021; FSB, 2017). The AI-based underwriting model leveraged by Upstart is an excellent Living Lab example: according to the US Consumer Financial Protection Bureau, Upstart employed alternative data and machine learning in credit underwriting and reported that its model approved more borrowers with a lower average Annual Percentage Rate (APR) than traditional models (CFPB, 2019; Upstart, 2019). This illustrates how predictive AI can enable financial inclusion by alleviating reliance on traditional and often scant credit bureau information.

But the benefits of this inclusion must be scrutinized. AI-enabled access to finance may create a variant of exclusion if customers are primarily assessed based on their digital footprints. The disadvantage could still hold for those with limited digital engagement, inconsistent employment histories, or atypical behavioral patterns. This introduces a tension between financial inclusion and what could be described as data-driven exclusion. AI can therefore open up access to some groups, but create behind-the-door barriers for others (Zetzsche et al., 2020). It is also important to highlight how dependent the output of AI is on the quality of input data, meaning biased or incomplete datasets, and how often it may lead to inaccurate and incorrect outputs. Hence, predictive AI by default doesn't. Without regular audits, tests, or explanations, it can perpetuate historical discrimination.

Moreover, predictive AI is at the heart of fraud detection and prevention against financial crimes. The use of Machine Learning Models can identify unusual transaction behavior way faster than manual monitoring systems. This is especially critical across the domains of digital payments, open banking, embedded finance, and cross-border flows of money, where transaction volumes exceed manual review capabilities for compliance teams. AI-empowered fraud systems can boost detection, lower false positives, and assist with real-time response (Arner, Barberis, and Buckley 2017; FSB, 2020). Many invested heavily in deploying machine learning tools to streamline their AML monitoring process and reduce volumes of inefficient alerts; for example, HSBC actually deployed off-the-shelf machine learning tech across its operations. Those thus have significant and sustainable cost advantages, as compliance functions are costly, labor-intensive, and liable to regulatory penalties in case of failures.

Generative AI injects an extra level of transformation. Predictive AI mainly predicts, while generative AI generates reports, summaries, policy drafts, customer communications, and synthetic scenarios, code, and even compliance documentation. Its applications could serve regulatory reporting, internal controls, customer support, legal review, stress testing, and knowledge management in financial services. Generative AI could transform risk and compliance functions as the technology automates, accelerates, and serves to augment tasks, from Compliance Monitoring to Climate Risk Analysis, argues McKinsey

(McKinsey, 2024). This is relevant because financial institutions need to cope with exponentially increasing complexity across AML, KYC, cybersecurity, consumer protection rules/sanctions screening/data protection/operational resilience requirements.

In the cost-effective perspective, both types of predictive and generative AI can help in lowering the cost of back-office functions, involving a lot of computations and compliance. Since global financial institutions pour billions into compliance, risk, and operational control, it is likely that automating document review, transaction monitoring, customer due diligence, and regulatory reporting could lead to significant savings (McKinsey 2023 + Arner et al 2017). This kind of logic is exemplified with cases like JPMorgan's COIN platform, where it was estimated that thousands of hours of manual legal and compliance work could be averted through AI-supported contract review (Nicoletti, 2021). But this also shakes up the workforce. Demand for some repetitive compliance and operational roles may decline with AI deployment, while demand for data scientists, model risk specialists, AI auditors, cybersecurity analysts, and regulatory technologists could increase.

Generative AI can drastically change not only the ways customers interact, but also how they find and adopt services. Some advanced AI assistants can respond to a diverse spectrum of customer queries with efficiency, clarifying products clearly and thoroughly, helping create seamless & personalized onboarding journeys, and even generating exclusive recommendations crafted according to clients' requirements in banks and FinTech enterprises. Today's trends point to chatbots and digital assistants as important use cases because they process human language and respond in real-time**.** For instance, AI supports robo-advisory in wealth management as AI will identify the investment portfolios that can be mapped to each user's risk profile, objectives, and preferences**.** For example, Betterment, Nutmeg, Vanguard, and BlackRock's Aladdin show how AI and automation are lowering the cost of investment advice and also extending greater access to low- income as well as young investors, putting pressure on traditional wealth managers to lower fees yet provide better digital experiences. (Nicoletti 2021)

Then, one indicator of such market disruption is through three channels. For instance, AI reduces operational costs, which means FinTech challengers can compete with incumbents without having an extensive branch network or legacy IT systems. Secondly, by significantly increasing scalability, AI allows platforms to serve millions of customers at very low marginal cost. Third, AI raises the level of personalization, enabling firms to create more tailored lending, investment, payments, and insurance products (Gomber et al., 2018). Ant Group, for example, is an ecosystem driven by AI that interconnects payments, credit scoring and lending decisions, wealth management, insurance, and risk management as features of a digital platform. This is indicative of platform economics with data, externalities, and ecosystem integration as drivers for competitive dynamics (Rochet & Tirole, 2003; Zetzsche et al., 2020).

Nonetheless, this same and inbuilt logic of the platform also generates an array of serious systemic problems and issues. The Financial Stability Board (2024) directly argues that the rising penetration of artificial intelligence-based systems in financial services gives rise to systemic vulnerabilities that are at once byzantine and somber. These vulnerabilities include, but are not limited to, model opacity (the majority of AI algorithm decision making remains inscrutable and interpretability), critical data dependency (over-reliance upon specific datasets for systems or models), dangerous risk concentration (many third party components become a de facto standard engines for many customers) making one point of failure across an industry, increased exposure

to cyber risks as the multiple vectors that can be attacked grow with wider adoption of AI technology on datacenter infrastructure and correlated behavior patterns between financial institutions deploying similar AI run models. Correspondingly, the European Central Bank has also noted that while AI use can bring considerable improvements to operational efficiency in decision-making arising from better data processing capabilities, they present a challenge to overall financial stability. This holds particularly true for cases where many institutions use the same or very similar algorithms, datasets, or cloud service providers, thus exacerbating systemic risk through homogenization (ECB, 2024). The macroeconomic implication of these observations is that while artificial intelligence facilitates agonistic competition and innovation at the microeconomic level, this further introduces systemic fragility and vulnerability at the world economic system scale, thereby fundamentally threatening financial stability.

Generative AI also presents unique reliability risks. This is very different than custom-built software, where a program must either certainly succeed or fail. In generative AI, the outputs can seem plausible, though they are actually wrong. Such “hallucinations” (McKinsey, 2024) would lead to legal, operational, and reputational repercussions when engaging in regulatory reporting or compliance advice. For example, a compliance report that fails to correctly interpret what the firm should be doing from a regulatory perspective could leave the firm open to sanctions. If a chatbot gives incorrect financial advice, it could be harmful for consumers. That is why generative AI calls for human touch, making the solution it generates auditable, validating, and ensuring clear accountability.

Cybersecurity is another critical issue. AI and ML systems perform valuable processing on a vast amount of information, making them an attractive target for malicious actors; moreover, AI itself can amplify the speed, accuracy, and scale of cyberattacks. AI can help defend against cyber-attacks using predictive capabilities to flag anomalies (predictive AI), but generative AI can also empower new waves of advanced phishing, synthetic identity fraud, and disinformation. Therefore, AI is two-fold: it increases defense and at the same time gives aid to offenses.

In summary, Predictive and Generative AI represent much more than an efficiency tool but are upending financial services, market competition, compliance, and regulation. They lower costs, widen access, and allow for greater customization of financial services. That said, those same methods also introduce risks regarding bias, explainability, cyber resilience, market concentration, consumer protection, and systemic stability. Ultimately, the value that AI will unlock over the long-term in finance is determined less by technology capability than governance: explainable models and ethical data use to robust cybersecurity, human accountability, and adaptive regulation.

2. Regulatory Challenges and the Role of RegTech

The combination of predictive and generative AI in financial services triggers multiple levels of regulatory concern that fall outside the domain of straight compliance. These challenges relate to data use, algorithmic accountability, consumer protection, market integrity, cybersecurity, and systemic stability. AI revolutionizes not only existing financial operations but also decision-making, risk detection, and regulatory supervision.

In line with institutional theory (DiMaggio & Powell, 1983), financial institutions implement AI-driven RegTech to a certain extent because of coercive pressure from regulation and interaction with various stakeholders to maintain legitimacy in a highly supervised sector.

As regulators expect faster reporting, stronger risk controls, and effective monitoring, banks, FinTechs, and payment platforms will continue to converge on similar AI-enabled compliance tools. AI-enabled financial ecosystems are multi-sided platforms from a platform economics perspective, wherein the value emerges through data, data-derived network effects, APIs, and scale of users (Rochet & Tirole, 2003). It makes regulation harder because financial activity might fold up inside a larger digital ecosystem instead of tucking neatly inside a regulated bank.

For just how expansive this transformation is, the global RegTech market is fueling strong growth, since more organizations must adapt to the growing regulations complexity, while large financial institutions are already investing very high sums each year on compliance, AML fraud prevention, reporting, and operational resiliency (McKinsey, 2023; Juniper Research, 2023). This makes AI look attractive as it promises faster monitoring, cheaper compliance, and better detection of malpractice. That said, this presents a regulatory issue as speed and automation may diminish human judgment where governance is ineffective.

2.1. Data governance, privacy, and consent

Data governance, privacy, and consent are one of the most significant regulatory challenges facing the adoption of predictive and generative AI in financial services. Predictive AI works with trillions of structured and behavioral data points to detect patterns, perform risk assessments, and help decision-making, while generative AI processes a massive volume of unstructured data, such as contracts, customer interactions, regulatory texts, and transaction records. This level of data dependence poses complex questions about data quality, informed consent, privacy protection, data retention, transparency and explainability, and cross-border data flows. APIs allow for secure, standardized access to customer data by third-party providers working within the open banking and embedded finance space, leading to innovation and competition. Yet this architecture also introduces more actors into play, handling sensitive financial data, thus heightening the threat of privacy infringements and cybersecurity risks, consent management challenges, and regulatory fragmentation across jurisdictions (European Commission, 2020a). This struggle is further evidenced by the introduction of Payment Services Directive 2 (PSD2), which, although opening the gates to information and financial innovation by giving Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP) access to customers' data, also increases the difficulty of governing this added complexity while hand-in-hand increasing security needs for oversight.

With the advent of AI, this challenge compounds further since data is no longer just a part of the transactional fabric but also an integral component in figuring out behavior, predicting creditworthiness, creating personalization models, and nudging decisions. This is where a data transparency gap emerges; consumers may not realize what happens to their data when reused or monetized across multiple financial functions at the same time. For example, data shared for account aggregation may be used later in credit scoring, fraud classification, or targeted financial products, all without the user being fully aware. External to the industry, the European Union formed one of the most comprehensive regulatory frameworks with the General Data Protection Regulation (GDPR), which focuses on aspects like lawfulness, transparency, data minimization, and user rights. In addition, the EU Digital Finance Strategy supports the establishment of a single financial data space and measures against risks posed by digital transformation (European Commission, 2020a). Most recently, the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) takes a risk-based approach to regulation and places ever

greater obligations on high-risk AI applications like credit scoring that affect access to financial services directly. The EU aims to strike a balance between innovation and significant consumer protection and ethical safeguards through the establishment of the first complete AI regulatory framework, as AI-enhanced financial decisions can have significant economic and social ramifications.

2.2. Algorithmic opacity and accountability

Algorithmic opacity is the second big regulatory challenge, of course. Predictive AI models, specific large machine learning systems, are often considered as “black boxes”. This is compounded by the fact that generative AI can generate outputs that, while plausible and convincing, are harder to verify. It is problematic for regulators, firms, and consumers.

One of the areas where this particular challenge exists is in credit scoring; if an AI model rejects a loan application, regulators must understand whether that decision was fair and explainable as well as formed on appropriate data. Consumers also need meaningful explanations. Companies can meet model performance standards technically, but not provide accountability without explainability. This is why the rise of explainable AI is at the heart of financial regulation (Zetzsche et al., 2020; BIS, 2021).

The Financial Stability Board (FSB) is an international body that monitors and makes recommendations to promote global financial stability. It was established in the 2009 G20 Pittsburgh Summit as a successor to the Financial Stability Forum (FSF). In that perspective, the Financial Stability Board says the speed at which AI is being adopted across finance, as well as a lack of data on how widely it is used through the economy, means that more attention by authorities is needed to improve monitoring and ensure supervisory frameworks keep pace. This arises especially as the AI risk is not confined to individual firms. Where many different firms use the same models, data sources, or even cloud providers, errors may be correlated across the system.

It also creates headaches for regulatory reporting. It can write reports, summarize commitments, and create compliance documentation. Though this is helpful, when the outputs contain errors or hallucinations, it becomes hard to hold anyone accountable. A company can not get away with blaming the model. The financial institution is still responsible for regulatory compliance. Achievement of this mandate will require firms to have accurate and complete audit trails, robust human review, and thorough validation processes, as well as clear and transparent model-ownership frameworks (McKinsey, 2024; FSB, 2024). These components are vital to ensure responsibility, improvement of precision, and upholding the integrity of models utilized in their operations (McKinsey, 2024; FSB, 2024). As a result, companies should expect to establish implemented frameworks that include comprehensive documentation of model construction/validation and deployment consistent with quality reviews by appropriately qualified personnel with well-defined responsibility for each model to help increase reliability and governance through the life cycle (McKinsey, 2024; FSB, 2024).

2.3. Consumer protection and financial vulnerability

The third most important challenge is the protection of consumers. AI can accelerate onboarding (internalize KYC & AML), enhance product personalization, offer robo-advice, and provide instant credit decisioning. But it can also unduly expose consumers to inadequate products, biased outcomes, or over-indebtedness.

The information from the ethical aspects of robo-advisory highlights multiple responsibilities digital financial platforms have, including disclosure, transparency,

consumer education, and limiting potential risks**.** What is directly relevant to AI? Robo-advisory platforms can help offer low-cost access to investments, but must ensure that investments are suitable given the user profile, risk tolerance, and level of understanding. Poorly designed AI-driven advice could cause consumers to misinterpret risks or create non-ideal positions.

Buy Now Pay Later (BNPL) and embedded lending are other great examples. AI is able to use behavioral and transaction data to approve credit instantly. While this enhances convenience and access, such a development may induce overborrowing if affordability checks lack stringency (FSB, 2022). Consequently, predictive AI can act as an inclusion mechanism but also as a risk multiplier in this context.

Transparency is also related to consumer protection. In a case where output from a chatbot, robo-adviser, or AI assistant is meant for communication with customers, it should be clear to customers who they are interacting with and if the outputs are regulated advice. This is especially relevant for vulnerable consumers. Ensuring that AI-driven personalization does not develop into AI-driven manipulation is the challenge of regulation.

2.4. Cybersecurity and operational resilience

Cybersecurity and operational resilience also face new challenges with AI. Cybersecurity is defined as: The practice of protecting digital systems, networks, and data from unauthorized access, theft, damage, or disruption. They also note that AI/ML can be used to aid cyber defense, but in the wrong hands, offensive adversaries are also leveraging it.

Data integrity is the crux of RegTech systems. AI systems that feed on biased training data, transacting data, or manipulating input-output of Models by the attackers will bubble up fake risk assessments. Generative AI could also help to carry out more complicated phishing, synthetic identity fraud, fake documents, and automate social engineering. What this means is that AI governance and cybersecurity governance cannot be siloed.

The FSB Identifies Financial Stability Risks Associated with AI, such as Third-Party Dependency, Cyber Risk, Model Opacity, and Data Concentration (FSB, 2024). The ECB likewise follows up on the opportunities for financing afforded by AI but cautions that extensive adoption in finance (including through widespread use of similar AI models or dependence on outsourced provision) "may provoke a risk to stability." These fears fit with the course point about cyber risk; connectivity means that economies are more susceptible to contagion through finance, payments, and infrastructure.

2.5. How RegTech improves transparency, supervision, and regulatory agility

As challenging as it may sound, RegTech comes with strong advantages. RegTech utilizes advanced technology and innovative digital solutions to enable firms to comply with regulations in a far more effective, yet remarkably efficient manner. RegTech combines new technologies and the latest software abilities to help organizations with their compliance process, execution speed, eliminate human error rate, and reduce operational risk. As a result, such incorporation of technology facilitates compliance with regulations more efficiently and assists firms in better understanding legal frameworks and resource utilization. AI-driven RegTech can improve:

- **Real-time transaction screening** for AML/KYC monitoring
- **Fraud detection** through anomaly detection
- **Automated data** extraction for regulatory reporting

- **Risk management** through predictive analytics
- **Market surveillance** through pattern recognition
- **Cybersecurity monitoring** through behavioral analytics.

This also greatly facilitates access to more timely, more detailed, and granular information, vastly increasing transparency and openness with regulators, as well as other financial firms. The compliance framework, as existing today, continues to be largely retrospective and passive: firms only aggregate their reports long after the proverbial horse has bolted; often in reaction to events that have occurred. Conversely, AI-powered Regulatory Technology (RegTech) can transform by enabling continuous and more real-time supervision and monitoring capabilities that could significantly strengthen the ability to identify potential risks much earlier than before they materialize into anything serious (Arner, Barberis, and Buckley, 2017; FSB, 2020).

ComplyAdvantage is a useful example. Its AI-driven AML solutions are focused on KYC screening, transaction monitoring, and real-time alerts for financial crime risk across institutions. Large Banks **like HSBC** are now adopting ML to ease AML monitoring by decreasing false positives. This is important because classic anti-money laundering (AML) systems usually produce huge numbers of false alerts that consume compliance resources and delay investigations.

RegTech also improves regulatory agility. Rule-based systems have trouble keeping up with new products: Cryptoassets, embedded finance, and AI-driven platforms. AI-enabled tools for compliance can adapt more quickly, spotting new forms of misbehavior or signals of risk. However, it needs to be mixed with validation. An ungoverned but fast system can lead to false confidence.

2.6. SupTech and the changing role of regulators

SupTech, or technology leveraged by supervisors to monitor effectively, is also gradually being adopted by regulators. This shifts regulators from being periodic reviewers to data-driven supervisors. Sandboxes, data analytics, and digital testing environments are utilized by regulators such as the Financial Conduct Authority(FCA) in London, the Monetary Authority of Singapore (MAS), or other authorities to familiarize themselves with innovation before firms become systemic/fails more broadly. The FCA protects and enhances the integrity of the UK financial system through judicious regulation of UK markets and firms, setting effective standards for their conduct, and holding both firms to account – with a clear consumer-centric focus on promoting healthy, laterally flowing markets supplying accurate prices derived from predictions that produce fair outcomes.

This shift is evidenced by the FCA Digital Sandbox. Instead of having to wait for innovation to be untested in the market, the sandbox allows firms to test solutions with regulatory engagement. It promotes innovation while mitigating regulatory uncertainty. Similarly, Singapore has also developed some principles for the responsible use of AI through its MAS : FEAT principles, to promote fairness, ethics, accountability, and transparency in the use of artificial intelligence and data analytics in Singapore's financial sector(OECD, 2025).

2.7. Comparison of global regulatory approaches

An international overview reveals three possible strategies.

The European Union (EU) is based on a comprehensive and rules-based approach. Open banking and payment initiation are regulated by the Revised Payment Services Directive (PSD2). Markets in Crypto-Assets Regulation (MiCA) establishes a comprehensive regulatory framework for Cryptoassets. The General Data Protection

Regulation (GDPR) regulates personal data. The AI Act comes up with risk-based obligations for AI. While this brings clarity and consumer protection, it can also be compliance burdens, especially for smaller FinTech firms (European Commission, 2020a; ESMA No Date; European Commission, 2020b).

The United States takes a less consolidated approach. Banks, securities markets, consumer protection issues, derivatives markets, and other financial crime are each overseen by multiple specialized, not generic or multi-purpose, regulatory agencies so that no chromosome-like mega-bureaucracy can evolve over any segment of the economy. It creates a decentralized regulatory framework designed to provide a flexible and dynamic environment that can cultivate innovation in the financial sector. This fragmented approach may lead to some regulatory inconsistencies, for example, leaving coverage gaps (e.g., some activities escaping adequate oversight) or creating unnecessary overlaps (e.g., multiple regulators applying duplicative requirements). As a result, AI governance in the United States financial system is generally characterized by a complex patchwork of sector-specific rules and regulatory tools, particularly FAQs and other supervisory guidance instruments, along with some established expectations around sound model risk management practices, in lieu of an overarching federal framework for law or regulation governing AI (FSB, 2024). Also, US policymakers try to figure out how they can protect the privacy of consumers while also protecting the interests and rights of consumers as those technologies are developed, so that all three systems work better. At the same time, it enables them to remain globally competitive vis-à-vis China.

In contrast, **innovation jurisdictions** such as **Singapore** chiefly maintain a high-level principles regulatory philosophy that focuses on controlled experimentation zones (i.e., sandboxes). These regimes place an emphasis on a close working relationship between the regulators and market participants, encouraging an interplay that strikes a balance of fostering innovation with sound risk management in the financial system.

MAS’s principles FEAT offers a flexible AI governance framework, whereas Singapore's sandbox approach incentivizes regulatory compliance when experimenting (MAS, 2018). Although this model is appealing for FinTech innovation, it needs to be supported by solid supervisory capacity and trust between regulators and firms.

In emerging markets, sandboxes are frequently employed to simultaneously promote financial inclusion as well as manage risks in developing or high-growth areas. This can work where you need to increase the access of people to payments, credit, and digital finance through innovation. Regulatory capacity may be more uneven, and data protection frameworks less developed.

It is a tightrope act to ensure that AI tools are not based on fragile or simply inadequate protections that undermine security and trust. Therefore, policymakers need to carefully balance the different lenses of regulation and economy while ensuring that new innovations and competitiveness do not adversely affect consumer protection and systemic resilience.

2.8. Critical evaluation

RegTech is not a panacea. That increases the speed of compliance efforts, but it also results in reliance on vendors and models as well as infrastructure. Another risk related to RegTech is that if a large number of institutions use the same tools, systematic weaknesses may be present across all those institutions. This is a problem of platform

economics: reaching scale and increasing standardization leads to efficiency but still creates concentration risk.

It is also capable of explaining a potential limitation of this theory, as institutions may perceive AI RegTech as an appropriate mechanism to maintain legitimacy, rather than one that they understand and desire to implement. Such an environment creates "compliance theatre," where institutions implement advanced systems in the absence of sufficient governance, auditability, or human expertise. This means that regulators need to closely monitor not just the use of AI by firms but also rigorously validate how reliable, transparent, explainable, or secure these tools are and if they have been properly designed for their intended purposes. Artificial intelligence poses unique, complex regulatory challenges around data use and control, transparency requirements, decision-making responsibilities, consumer protection measures, cybersecurity defenses, and overall system stability. In this regard, RegTech and SupTech are becoming more important as they complement supervision with advanced tools for continuous monitoring, automated and precise reporting, and predictive analysis to identify possible risks or threats in advance. But their success is contingent upon governance, explainability begrudgingly, and the human and international coordination. Regulators will play a larger role for ecosystems, models, data flows, and technology providers than just licensed financial institutions in the future

3. Case Studies: AI in Financial Services and RegTech

Lastly, a multitude of compelling real-world case studies strongly demonstrates that predictive and generative artificial intelligence is no longer primarily a theoretically or academically related technology but has already made meaningful inroads into key high-impact use cases across many areas such as compliance monitoring, regulatory supervision, detection and prevention of financial crimes, credit evaluation and scores embedded finance applications for credit scoring based on savings account deposits (Jiang Zhang et al., 2022a), innovative regulatory experimentation activities. But at the same time, these illustrative examples highlight not only an inconvenient truth that much of what is required for successful AI implementations rests upon several fundamental pillars, whose critical importance resonates most strongly in areas such as governance, transparency and accountability, data quality and reliability in dynamic populations over long periods of time rather than static conditions, clear explainability of complex decisions powered by machine learning algorithms, and also a perspective that differs significantly from those exaggerated claims made by companies once hailed as innovators. The following case studies reinforce the central thesis that AI produces efficiency triumphs as well as new regulatory weaknesses.

3.1. HSBC and Google Cloud AML: predictive AI in financial crime compliance

One of the most powerful applications of predictive AI is anti-money laundering (AML), and HSBC provides one of the strongest examples. These systems are highly dependent on preset static rules that create a large number of false alerts. That ratchets up compliance costs and can lead investigators down rabbit holes where it is not really suspicious behavior. An example of machine learning applied to transaction movements, network behavior, and KYC data used in HSBC to score better risk outcomes is the AI-powered AML tool developed by Google Cloud. According to reports, the tool was able

to cut HSBC's alerts by about 60% and boost its true positive detection rates two- to fourfold (Google Cloud, 2023; Investopedia, 2023).

This case demonstrates the operational value-add of predictive AI: that it can provide significant compliance efficiency in detecting and identifying fraud while decreasing reliance on time-intensive manual investigation processes. This highlight, however, reflects a point of regulatory tension. AML systems have to be sufficiently explainable for regulators to see why some transactions are flagged and others are not. In the case where we cannot completely audit and test an AI system's complex decision-making paths, it becomes almost impossible to trust a model even with better accuracy and more advanced prediction capabilities. HSBC has previously faced severe regulatory sanctions for weaknesses in its anti-money laundering (AML) controls, including a fine issued by the UK Financial Conduct Authority (FCA), directly attributable to shortcomings in transaction-monitoring systems (FCA, 2021; The Guardian, 2021). So, the real verification and validation of compliance and reliability of AI technologies can only be assured if they are combined with strict, comprehensive model governance frameworks, meticulous, transparent audit trails, as well as clear systems of human accountability and oversight.

3.2. JPMorgan COIN: generative and analytical AI in legal and compliance automation

A terrific example of how AI might automate complex legal and compliance work comes from JPMorgan, which has a platform called Contract Intelligence that is commonly referred to as COIN. BigQuery: The same year, a system was trained to review commercial loan agreements and extract important clauses in order to avoid manual review that took 360,000 hours of work annually (Nicoletti, 2021; JPMorgan, 2017). Through the RegTech lens, this is very relevant since financial institutions are mired in documentation, contract review, and reporting requirements.

This not only significantly reduces cost because of decreased inconsistency and faster compliance processes, but it also allows using AI to enforce rules in a scale-up manner. But it also reveals the limits of automation. Legal and regulatory interpretation requires judgment, context, and accountability. If a contractual clause is misclassified or an inaccurate compliance summary is generated by AI, the institution still bears responsibility. The real question for regulators is not whether AI can quickly process documents, but whether the outputs of those systems are reliable, auditable, and explainable to a human. Thus, this case therefore backs up the contention that generative and analytical AI improve compliance efficiency but not govern responsibility.

3.3. Ant Group: platform AI, systemic risk, and regulatory intervention

Ant Group is the quintessential (and most extreme) example of AI+platform finance. Using Alipay and related services, Ant Group created a digital ecosystem that combined payments and lending, credit scoring, wealth management (through mutual funds), and even insurance. Its AI models utilized data from the platform to evaluate customer behavior and creditworthiness, thereby broadly increasing access to digital lending at scale (Zetzsche et al., 2020). This architecture of Ant's ecosystem demonstrates platform economics: the more users and transactions it commands, the more data it generates, which in turn strengthens its capabilities to customize services and assess risk.

But it also raised acute systemic issues on that kind of scale. Before Ant Group's IPO, Chinese regulators stepped in for financial stability, consumer protection, leverage, and

other data governance concerns. It simply worked on signaling that technology firms providing financial services cannot operate out of prudential expectations by virtue of their being a platform structure. However, it was also reactive. Before the intervention, Ant was already at systemic scale. The key weakness common in many regulatory systems is that, as supervisors are often too far behind the curve, following the accumulation of systemic risk on platforms. It supports the argument that regulators require earlier SupTech to monitor rapidly evolving AI-based financial ecosystems.

3.4. Upstart: AI credit scoring, financial inclusion, and fairness concerns

Upstart is a great example of predictive AI in consumer lending. The company harnesses machine learning, as well as alternative data across "alternative applications" around education and employment-related events for credit underwriting. The No-Action Letter for Upstart was issued by the US Consumer Financial Protection Bureau in recognition of its use of alternative data and AI in a lending decision (CFPB, 2019; CFPB, 2020). Upstart claims its model approved 27% more borrowers than traditional models, and the APR was lowered by an average of 16% on loans they approve (Upstart, 2019).

This analogy reinforces the access argument: predictive AI can broaden access routes for consumers who would be excluded by more restrictive credit scoring models. But should it also trigger serious regulatory questions? If any of the variables, such as education, employment history, or digital behavior, correlate with protected characteristics, alternative data may end up indirectly reproducing social inequalities. The innovation with the regulatory response was that CFPB employed its no-action letter approach in a controlled way that allowed experimentation, all of which needed to be monitored. But its success will depend on ongoing evidence, fairness, and transparency. Upstart demonstrates that AI can bring greater access than a human (in this case, the loan officer), but inclusion only grows to the extent regulators can confirm there is no overt or covert discrimination hidden in small amounts of every group's subprime lending pie.

3.5. Klarna and BNPL: AI-driven instant credit and consumer protection

An example of how AI can assist in getting instant credit decisions right into the e-commerce journeys is Klarna’s buy now, pay later. It allows you to analyze risk, detect fraud, and even offer personalized credits in a faster way. This makes it more convenient and may open up additional short-term credit channels. But it also brings up consumer protection issues. BNPL is integrated at checkout, so consumers feel like a creditless purchase, like that seamless purchase feature, and not debt. This raises the potential for customers to over-borrow, especially for younger or financially vulnerable customers (FSB, 2022).

In the UK and EU, regulatory responses already tend to target affordability checks, transparency, and assessments of creditworthiness. These are the responses that are needed and have generally remained out of step with market growth. Example: Klarna. To show how AI-enabled embedded finance can intertwine commerce and credit, consider the case of Klarna. Regulatory takeaway: Design products with consumer protection incorporated, rather than as an afterthought on a dysfunctional product once harm has happened.

3.6. Stripe: AI-driven fraud detection and embedded finance infrastructure

Predictive AI in global payments and embedded finance by Stripe. Stripe Radar, its fraud detection system, employs machine learning on massive amounts of transaction data to flag suspicious activity and reduce merchant fraud. It is a textbook case of platform economics: Stripe's worldwide payment network results in data that enhances its fraud

models, which leads to additional merchants forcing the platform (Rochet & Tirole, 2003; Gomber, Koch, and Siering, 2018).

Cross-border oversight is the regulatory challenge. Stripe assists merchants with cross-jurisdictional operations, where AML, data protection, and consumer protection, as well as payment rules, may vary from one market to another. This is where AI may come in to help manage the complexity, but regulators need to ensure platform-based fraud systems avoid morphing into opaque private infrastructures that fall outside of any meaningful supervision. The example of Stripe highlights how AI enhances market efficiency but also creates the potential to centralize operational power with payment infrastructure providers.

3.7. ComplyAdvantage: AI-powered RegTech for AML and sanctions screening

For example, ComplyAdvantage is a direct RegTech case. It provides real-time AI and machine learning financial crime risk intelligence, AML screening, transaction monitoring, and sanctions alerts. This tool enables firms to discover suspicious behavior more quickly, resulting in faster and better compliance (Arner, Barberis, and Buckley 2017). It is particularly advantageous for FinTechs and payment providers that require scalable compliance capabilities but do not wish to develop big in-house compliance teams.

On the other hand, RegTech's effectiveness relies on the quality of data, model governance, and explainability. An incomplete or biased risk intelligence leaves firms vulnerable to missing high-risk activity and misclassifying customers. So ComplyAdvantage demonstrates what is both the promise and the limitation of RegTech: increased compliance agility, but not institutional absolution. Firms are still expected by regulators to understand and govern outsourced or third-party compliance tools.

3.8. FCA Digital Sandbox: AI supervision and regulatory experimentation

8 FCA Digital Sandbox Illustrating a shifting landscape for regulators responding to AI-enabled ways of accommodating end-user finance. According to the FCA, its Digital Sandbox offers data sets that are compliant with GDPR as well as a safe environment in which firms can test and scale proofs-of-concept (FCA, 2025). Mentorship stats based around six theme areas play another role here, facilitated through integration into the FinTech ecosystem. This indicates a shift from a purely reactive regulation to more collaborative supervision.

They make up for it with a sandbox model that works precisely because regulators watch innovations reaching the market at full scale. In addition to giving controlled data environment access, it assists in minimizing the uncertainty present for small firms. Sandboxes are, however, not a perfect fix. They are tested at reduced conditions and then risk endemic results that may be incompletely portrayed after product use. As such, the effectiveness and efficiency of FCA models are maximized when integrated into a more holistic SupTech framework. This all-encompassing approach combines a continuous process of live monitoring along with extensive post-authorization supervision and thorough model-risk governance frameworks to create a dynamic regulatory ecosystem.

3.9. Critical synthesis

These case studies together showcase four insights. In a nutshell, predictive AI helps with compliance and the governance aspect of risk management in three areas, namely AML, fraud detection (KYC), and credit scoring. Second, generative and analytical AI will

reduce legal and compliance costs but need strict controls to eliminate incorrect or untraceable outputs. Third, as seen with AI-driven platforms like Ant Group, Stripe, and Klarna, one of the largest risks is that regulatory threats will come when finance becomes embedded inside massive data ecosystems. Fourth, while regulatory responses are becoming more nuanced and effective, many of these measures remain reactive – addressing issues post-hoc as opposed to anticipating and stopping them from happening. So, the answer I think is not to ban AI but rather to create governance systems and a whole ecosystem of risk mitigation to include requirements such as transparency through explainability, auditability from both internal mechanisms and independent external bodies, cybersecurity resilience for malicious attacks, consumer protection through transfer and storage policies; ongoing, longitudinal supervision or other mechanisms that allow enough monitoring of capabilities over time. These cases show that the role of AI to produce value from RegTech relies less on automation per se, but rather on whether this automation is subordinated to accountable governance.

Conclusion

As both predictive and generative AI, artificial intelligence is already fundamentally disrupting the core of finance, not only the ways firms deliver a multitude of different financial services, but even changing the markets themselves on which they rely. These technologies improve operational efficiency, significantly reduce transaction costs, and broaden access to a wide range of financial products and services. However, in parallel with these significant enablers, they introduce material and multifaceted governance, fairness, and system stability risks that need to be addressed.

Although these challenges can be complicated and sometimes daunting, they also represent significant, emerging opportunities to facilitate the development of diverse new technologies referred to as the family of Regulatory Technology (RegTech) and Supervisory Technology (SupTech). These advanced tools allow regulators to monitor compliance in real-time, paving the way for proactive, rather than reactive supervision. However, the value and capabilities that RegTech and SupTech can truly yield rely on sound governance frameworks that are closely linked to well-crafted, future-oriented, and strategically implemented regulatory policies.

The challenge of achieving balance between enablement and stability will be the central determinant in shaping how financial services evolve globally. Striking this perfect balance requires building out and deploying a set of critical building blocks, including:

- Regulatory frameworks that are highly adaptable and flexible enough to evolve while technology evolves;
- Ensuring that we have robust cybersecurity strategies and practices in place to safeguard sensitive financial data and systems against an increasingly sophisticated range of cyber threats;
- Worked with global regulators to align standards and policies across jurisdictions, reducing the risks of regulatory arbitrage and fragmentation.

In the long run, AI will likely not only transform the provision and reach of financial services but also redefine traditional regulatory functions and responsibilities, altering the structure of the global financial system itself. At the same time, the greatest challenge and most important litmus test of successful financial innovation, especially in light of the impending sustainable transition, will be making sure that these innovations are designed

and implemented inclusively, governed transparently, and resilient enough to survive future shocks or ambiguities.

References

Arner, D.W., Barberis, J. & Buckley, R.P. (2017). *FinTech and RegTech: Impact on regulators and banks*. Journal of Banking Regulation.

Bank for International Settlements (BIS) (2021) *Artificial intelligence in finance: Opportunities and challenges*. Basel: BIS.

Consumer Financial Protection Bureau (CFPB) (2019) *No-action letter to Upstart Network, Inc.*, Washington, DC: CFPB.

Consumer Financial Protection Bureau (CFPB) (2020) *CFPB innovation programs and AI in lending*. Washington, DC: CFPB.

DiMaggio, P.J. & Powell, W.W. (1983). 'The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields', *American Sociological Review*, 48(2), pp. 147–160.

European Central Bank (ECB) (2024). *Artificial intelligence and financial stability*. Frankfurt: ECB.

European Commission (2020a). *A digital finance strategy for the EU*. Brussels: European Commission.

European Commission (2020b). *Proposal for a regulation laying down harmonized rules on artificial intelligence (AI Act)*. Brussels: European Commission.

European Securities and Markets Authority (ESMA) (no date) *Regulation of financial markets in the EU*. Available at: https://www.esma.europa.eu

Financial Conduct Authority (FCA) (2021). *HSBC fined for anti-money laundering failures*. London: FCA.

Financial Conduct Authority (FCA) (2025). *Digital Sandbox overview*. London: FCA.

Financial Stability Board (FSB) (2017). *Artificial intelligence and machine learning in financial services*. Basel: FSB.

Financial Stability Board (FSB) (2020). *The use of supervisory and regulatory technology by authorities and regulated institutions*. Basel: FSB.

Financial Stability Board (FSB) (2022). *Regulation of Buy-Now Pay-Later services*. Basel: FSB.

Financial Stability Board (FSB) (2024). *Artificial intelligence and financial stability: Risk analysis*. Basel: FSB.

Gomber, P., Koch, J.-A. & Siering, M. (2018). ‘Digital finance and FinTech: Current research and future research directions’, *Journal of Business Economics*, 87(5), pp. 537–580.

Google Cloud (2023). *HSBC AML transformation using artificial intelligence*. Available at: https://cloud.google.com

Investopedia (2023) *HSBC adopts AI for fraud detection*. Available at: https://www.investopedia.com

JPMorgan Chase (2017). *COIN: Contract Intelligence platform overview*. New York: JPMorgan.

Juniper Research (2023). *RegTech market forecast report*. London: Juniper Research.

McKinsey & Company (2023). *The future of risk and compliance in financial services*. New York: McKinsey.

McKinsey & Company (2024). *The economic potential of generative AI in banking*. New York: McKinsey.

Monetary Authority of Singapore (MAS) (2018) *FEAT principles for fairness, ethics, accountability, and transparency in AI*. Singapore: MAS.

Nicoletti, B. (2021). *Artificial intelligence in financial services*. Cham: Springer.

Rochet, J.-C. and Tirole, J. (2003). ‘Platform competition in two-sided markets’, *Journal of the European Economic Association*, 1(4), pp. 990–1029.

The Guardian (2021) *HSBC fined over anti-money laundering failures*. Available at: https://www.theguardian.com

Upstart (2019) *AI lending model performance report*. Available at: https://www.upstart.com

Zetzsche, D.A., Buckley, R.P., Arner, D.W., & Barberis, J.N. (2020). *Decentralized finance (DeFi)*. Journal of Financial Regulation.

LIBF (no date) *Topic 5–8 course materials on AI, cybersecurity, and regulation*. London Institute of Banking & Finance.