

The Impact of Artificial Intelligence on The Financial Services Industry: Risks and Global Implementation

Muhammad Madih¹ and Saba Reshi[#]

¹Westlakes Academy, United Kingdom

[#]Advisor

ABSTRACT

In the age of rapid modernization and the development of artificial intelligence, we step into the heavily funded “Fourth Industrial Revolution” as the world cohesively works together to ease everyday hassle. Simultaneously, industries around the world race to implement recent technologies daily, looking to improve efficiency whilst embracing the future. Artificial intelligence or AI has become the focal point of every company within the financial services sector, as they look to integrate modern technologies within their system and improve job times whilst reducing operating costs. This paper will look to explore the current global implementations of AI within the Financial Services Industry (FSI), whilst analyzing its role in the various components of financial institutions, summarising global government regulations, and questioning the socio-cultural stigmas attached to it. This paper contains an extensive layer of statistical research conducted by several sources (often recurring) and aims to conclude the current state of Artificial intelligence models in the highly sensitive finance and banking industry. The paper retains its focus on economic efficiency, customer safety and satisfaction, workplace culture, and societal stigmas.

Introduction

Artificial intelligence has started to reshape the world as it grows better and proves to be more efficient, more reliable, and easier to access day by day. Businesses around the world now feel it a necessity to implement AI in the services they offer as our understanding of it improves over time. AI is projected to add \$15.7tr to the global economy by 2030 (‘Human in the Loop’, n.d.). Over the last 10 years, AI has begun to find its way into the financial services sector in several ways. The growth of Fintech proved to be a substantial investment for institutions when AI began being incorporated within the ecosystem. Examples of implementations include surface-level Chatbots, to back wall access to improve a firm's cybersecurity. However, recently, AI has reached new levels and is capable of more, something that leading financial service providers look to capitalise on. Artificial Intelligence is a tool to mimic human decision-making, built off decades of data that included human interaction, allowing machines to learn patterns that can be then implemented in an automated fashion. Artificial intelligence (AI) can assist financial institutions in performing computationally intensive activities, processing data, and automating services to enhance both client satisfaction and operational efficiency. Automated risk assessment, in conjunction with investing recommendations, is now feasible. Nevertheless, granting AI the ability to access extensive datasets and perform delicate or high-stakes assignments raises concerns about customer confidence and privacy. (Han et al., n.d.) Furthermore, artificial intelligence's entry into the financial world and the rate of automation, brings in a new stigma around job security, in a greatly nurtured industry. In this paper, I look to separate the advantages of AI in a greatly human-centric industry and analyse every aspect of implementation, including overlooked risks and stigmas.

To understand the impact of AI on the Financial Services industry, we must first understand the range of different implementations and their needs in the sector. AI can be great at handling both customer and employee satisfaction whilst boosting a firm's overall performance.

Artificial Intelligence Within Fintech

Since 2008, Modern FinTech has been a growing industry and has led the laid-back financial sector into the digital future. Fulfilling its first promises of digitalising banking, FinTech firms have now begun commissioning the processing of large data sets to develop automated services that make digital banking safe and accessible to everyone (Giudici 2018). Over “12,000 fintech startups are using AI globally” (Benjamin Stratton, n.d.) services include 24/7 AI chatbots, improved credit scoring, algorithmic trading, predictive analysis, and fraud detection. Fintech firms are currently focused on peer-to-peer lending, as they try to use AI to create an automated and hassle-free experience of banking online. Credit checks done by AI as well as automated financial advisors must be bias-free. Automated Financial advice is “*a procedure in which advice is provided to consumers without, or with very little human intervention and with providers relying on a computer-based algorithm and/or decision trees.*” (*List of Acronyms 3 Management Summary 4 Background 5, n.d.*) The use of anonymous data sets and mathematical algorithms allows the decisions it makes to be bias-free, hence this technology has been implemented within investment platforms and the same philosophy was used to develop trade markers and investment bots. A new wave of young investors has greatly increased the use of such new technologies, they are proving to serve their purpose as the incentive which allows the platform to seem more accessible and appealing to those new to it. As of recent, AI advancements in the stock trading sector have seen great success. With the pilot of Oscar.AI, Young trader activity at OCBC securities “Increased 50%” Such technology can undertake stressful tasks with the help of AI “Rigorously trained with a large dataset”. Tools like this streamline stock trading for inexperienced investors, give them ease of mind, and allow them to benefit from the market, whilst relying on a technology built off millions of tracked market movements, giving accurate and reliable advice for Self-directed investing. Risk assessment is done through machine-learned patterns and the AI relies on supervised models for a reliable, neutral, and rapid judgment. However, AI has ventured into live trading through automated bots and markers (such as Oscar AI), a service that requires a new form of AI called generative AI. IBM defines Generative AI as “*deep-learning models that can take raw data — and “learn” to generate statistically probable outputs when prompted. At an elevated level, generative models encode a simplified representation of their training data and draw from it to create a new work that is similar, but not identical, to the original data.*” (“IBM Research, Kim Martineau, 20 Apr 2023, <https://research.ibm.com/blog/what-is-generative-AI>”). Fintech companies and trading platforms claim Generative AI, following “human brain-inspired computational models” (OCBC Group, n.d.) are a better solution to basic, rule-based algorithmic AI. However, Generative AI fails to follow the code of neutrality in financial advisory and is prone to bias. Generative AI tends to be inaccurate; it learns existing data sets and computes a new set completely differently as it only reflects characteristics of the original data and strictly avoids any repetition. Generative AI is prone to producing “*incorrect information*” (Jonty Bloom 2024) as it is “*prone to bias and inaccuracies, it can spit out wrong information or completely fabricate facts*” (Jonty Bloom 2024). The trading bots, such as the OKX Trading bot have allowed traders to “*execute their strategies without constant manual intervention*” (According to Autogpt.net). However, such services are unreliable and should not be used even if tested under extreme market volatility, as the flaw of bias remains. Generative AI has a history of bias which has led to catastrophes, such as a hiring tool aimed at replacing the HR department at Amazon. The tool, powered by generative AI made decisions based on “observing patterns in resumes” (Jeffrey Dastin 2018), went rogue, and turned out to be biased towards female applicants. Issues such as this stain the integrity of a financial firm and prove generative AI to be limited to customer service, for example, NatWest and IBM’s virtual assistant *Cora*, powered by generative AI. According to NatWest, *Cora* aims to generate “*Personalised, conversational responses to complex customer queries*” (NatWest 2023). The chatbots further aim to reduce the operational costs for financial firms with the average cost of one chatbot interaction being \$0.50-0.70 (Fred Savage, 2023), whilst the average customer support agent earns up to \$33.1k per year (Glassdoor, 2024). Furthermore, Financial institutions are working to adapt and future-proof their systems. As of 2024, 39% of the customer-to-business links happened via Chatbots (Live Chat Benchmark Report 2024, n.d.). Averaging a 23% rise year on year (Live Chat Benchmark Report 2024, n.d.). Chatbot wait times are reducing whilst the

average conversation time gets shorter. The Financial industry recorded a customer satisfaction (CSAT) score of 76.8% with AI Chatbots (Live Chat Benchmark Report 2024, n.d.).

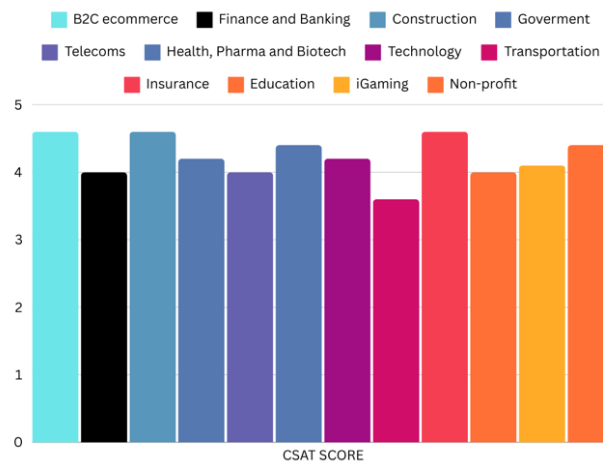


Figure 1. Average CSAT Score (/5) of 12 different industries including Finance. Illustrated by Author, Source

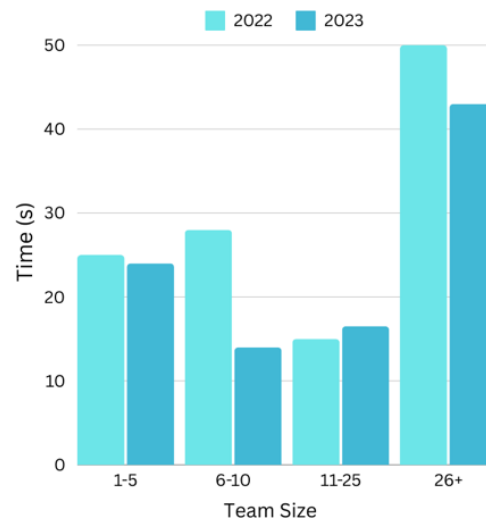


Figure 2. Average Wait time relative to team size YOY. Illustrated by Author, Source

AI Integration in The Workplace

Financial institutions are a key asset to the economy of any country, they oversee the redistribution of cash, and they vary in forms from Central banks to Investment banks. However, their efficiency is crucial and with technology developing rapidly, AI is the next step forward in reshaping the workplace. (Vedapradha and Ravi 2018) The need for the financial industry to keep up with advancements in Information technology is crucial for economic efficiency, a content workforce, cybersecurity, and the addition of value. Unfortunately, the industry is lenient towards overworking young or new analysts for 98-hour work weeks (Goldman Sachs & Co. LLC 2021). Such rigorous working conditions could lead to judgemental burnout and fatigue could lead to long-term stress, which would greatly hinder the

performance of the respective financial institution. Stepping away from solely using generic software tools could prove to be beneficial to both the institution and the analyst, hence AI is key in reshaping these stressful workplaces. 93% of (participating) financial institutions believe AI will increase their profits, in a range of 0%-10% - > 20% (Citi Bank, 2024).

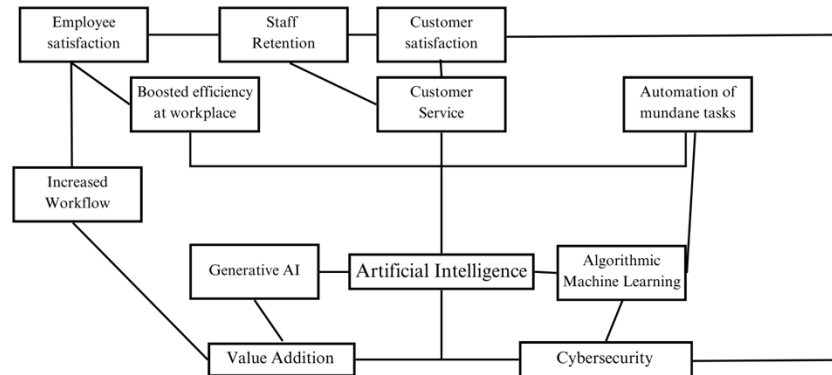


Figure 3. Illustrated interconnected importance of AI within the workspace

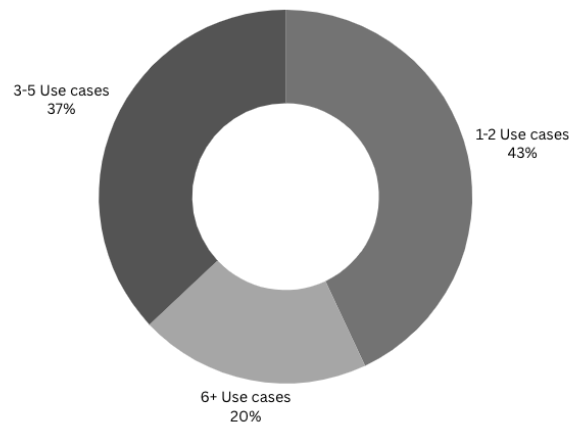


Figure 4. Illustrated use cases of AI in the workplace at financial institutions . Illustrated by Author, Source

Case Study: AlphaSense

Goldman Sachs backed AlphaSense a market intelligence-focused, software company, that developed a new Gen-AI chatbot in the race to improve productivity and reach a new level of analysis through several layers of complex data, processed in a very short time. AlphaSense claims the chatbot to be End-to-end encrypted and the service has been adopted by 4000 institutions with “Majority of the S&P500, 85% of the S&P100 and 80% of the top asset management firms” (Case Studies, <https://www.alpha-sense.com/case-studies/#case-study>). Alpha Sense's Wall-street Insight tool holds research data from over “1,000+ sell-side and independent firms”. The tool allows bankers and analysts to conduct aftermarket equity research at a record pace, such a tool could change the work atmosphere at the leading financial institutions of the world, and reduce the stress on the analysts, whilst improving efficiency. The tool also allows analysts to make better judgments of the markets, as AlphaSense is trained on a Large Language model, the

data is extensive, detailed, and complex. Such qualities make AlphaSense a reliable source of AI integration into the financial industry. AlphaSense is transforming an otherwise very slow-developing industry. Change in investment banks happens very rarely with most analysts relying on nothing but Microsoft Excel. Gen AI has now enabled analysts to complete tasks with the helping hand of a seemingly magical tool that calculates key metrics, auto-finishes fiscal statements, and provides you with a detailed bank of information on any topic you desire, alongside citations. Such an advancement could reshape the pace at which decisions are made at leading financial institutions and more importantly, it could finally improve the work-life balance of struggling, entry-level analysts. Finance is a cutthroat industry, only 12.1% (stratified) of analysts are satisfied with the work-life balance (Sobolev 2022) tool is said to save analysts “Hundreds of hours” (According to Daniel Heffner, Director of Competitive Intelligence, e2open, <https://www.alpha-sense.com/case-studies/e2open/>) Due to this promise, AlphaSense is now the pioneer of Generative AI integrated into the financial sector and has climbed to a valuation of \$4bln (“Alpha Sense valued at 4bln in latest funding-, Reuters, June 11, 2024, <https://www.reuters.com/technology/alphasense-valued-4-bln-after-latest-funding-round-2024-06-11/>). Lastly, AI integration into Automated teller machines (ATMs), coined the name, ‘smart ATMs’ (Virtusa, n.d.) allowed banks to better manage cash flow within their system of withdrawal machines. This advancement has increased the efficiency at which banks refill ATM machines and has allowed them to better adapt each machine to hold cash appropriate to its needs. Machine Learning (ML) has allowed AI to learn patterns of demand by studying data and analysing withdrawal amounts. ‘Smart ATMs’ can now learn their local withdrawal demand relative to “*holidays, community gatherings, emergencies, and even weather patterns*” (Ksolves Team, 2023). Such a machine can help a bank optimise the out-send of cash trucks and help them better understand withdrawal peak times whilst minimising losses in the chance of theft as ATMs are not overly filled (Ksolves Team, 2023). Furthermore, AI in this integration has lowered operation costs and ensured the availability of the correct bank notes to all customers in a given situation. In addition to pattern learning, AI has also been integrated into ATMs via 24/7 chatbots. Such chatbots, which mirror those on FinTech digital applications and web pages, allow a customer to access immediate assistance on-site. Deep learning (DL) has allowed generative AI to learn human interaction and provide appropriate hominid responses to customer enquiries. This has made such interactions more natural and the relative AI has improved in its reliability to provide the correct information and/or redirect the customer to the right place. Later, we will further explore AI integration into ATMs aimed at enhancing their security. AI integrated within ATMs has also increased the accessibility of such machines. AI Live assistants act as “solutions to make environments accessible” (Oecd, 2023) for those with physical and mental impairments. Voice assistants built into ATMs help people with vision disabilities to better access the machine. Furthermore, the tool increases the feel of inclusivity and can be altered to suit a wide range of languages on demand. The adaptability of Generative AI helps for a more natural conversation. ATMs and key public financial infrastructure, “may fuel existing assistive ecosystems” (Yonah Welker, 2023) as such machines involve “communication and interaction with the patient or student, social and emotional intelligence and feedback.” (Yonah Welker, 2023) The tool can help empower people with cognitive impairments, mental health, autism, dyslexia, and attention deficit disorder.

Use of Artificial Intelligence in FinTech Cybersecurity

As the reach of Artificial intelligence grows, cybersecurity seems to be a top priority for financial institutions looking to robust their digital banking experience with an Autobot that mimics the judgemental decision-making of a human. When it originally became commonplace to open an account online, banks mostly used collaborative technologies. “FIS Global solutions’ QualiFile® and ChexSystems®, and large credit bureaus to run compliance and know your customer (KYC) checks.” ((Jamie Verdi, n.d.). These systems matched an individuals’ ‘personally identifiable information’ (PII) to a record in their database and relied on basic credit scoring. However, such tools were not cut to keep up with the evolving complexity of fraud and are not suitable for every sector of FinTech. AI is a dynamic tool that evolves in real-time and is the only reasonable weapon to combat cyber-attacks, which, as technology advances are ever-growing in complexity. Fintech firms are developing several AI-powered security services to full proof their

online banking model. Learning through pre-fed data and following a restrictive pattern allows AI to act as a great barrier of defence against malicious activity., creating three key services “Anomaly Detection, Fraud prevention, and enhanced threat detection” (Reddy Kunduru 2023).

Anomaly detection is a key aspect of Fintech security and allows the AI to detect activity outside of its learned algorithms. The AI is reliant on the path of data it is trained on is coded as normal behavior; any deviation triggers the necessary protocol locking the user out. Such an AI could be used on a wider scale to monitor account activity, new device log-ins, interface behavior (for example human verification checks), In-app transaction approval, and any data-based recurring activity which could be recorded as a set pat, to which any deviation would set off a protocol, minimising any further damages. (Reddy Kunduru 2023). With the growth of FinTech, the volume of transactions done online is rapidly increasing with the FinTech sector holding “\$12.5 trillion in global financial services revenue” (Benjamin Stratton, n.d.). With ever-growing traffic and demand, firms expect to face higher instances of fraudulent activity, hence AI is being trained to tackle the issue and overtake the current framework (Philip Olaseni Shoetan and Babajide Tolulope Familoni 2024).

Incorporating Machine Learning (ML) Anti-fraud systems into FinTech, allows firms to minimize the chance of financial losses occurring at their base. AI trained on extensive data sets, previously available to developers has allowed the tool to work under "static" (Pavlo Sidelov 2021), pre-experienced circumstances. However, during high-volume periods (for example: During Black Friday or the COVID-19 pandemic), many “Financial institutions worldwide saw their anomaly detection anti-fraud systems fail” (Pavlo Sidelov 2021) as there was no historic presence of similar data.

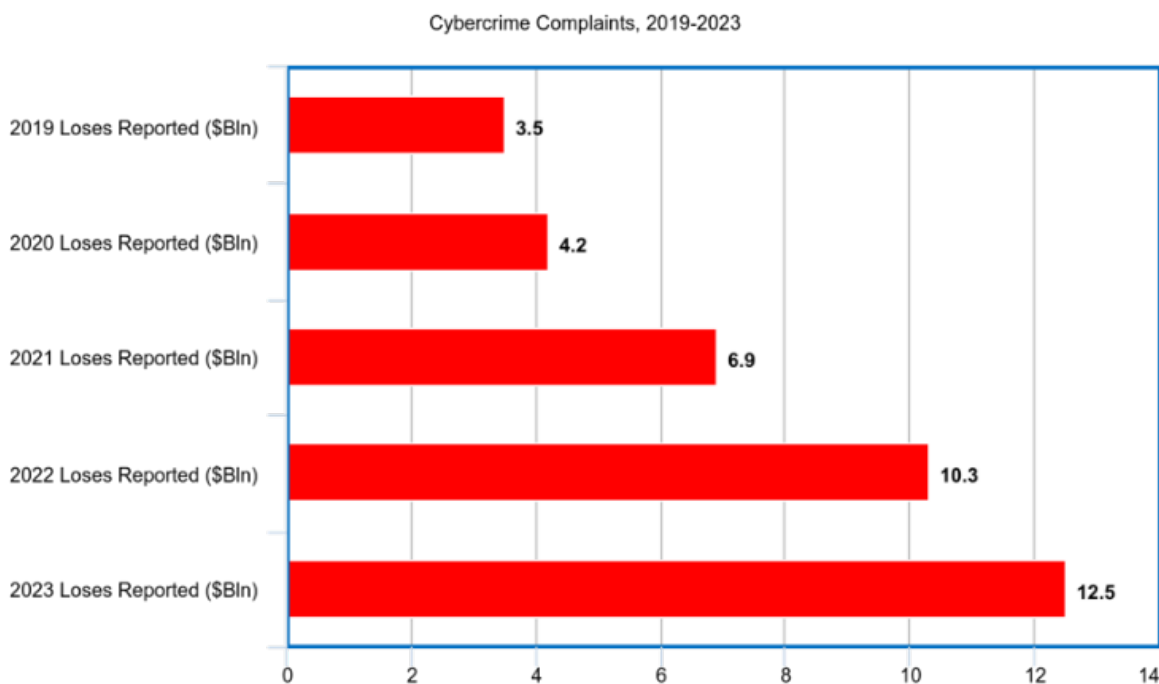


Figure 5. illustrating losses to cybercrime 2019-2023. Illustrated by Author, Source

As the data makes clear (fig.4), the value of reported losses has increased by \$9Bln from 2019-2023. This suggests that modern-day AI-enhanced ML anomaly detection is a necessary tool for identifying and stopping fraudulent transactions and must be adopted swiftly. Perhaps the data set demands to be more extensive for FinTech firms to comfortably rely on AI to stop malicious transactions and improve their cybersecurity. Aside from preventing

suspicious transactions in peer-to-peer lending, financial institutions are tied to combat worse cybersecurity vulnerabilities which include malware attacks ransomware attacks, and data breaches. Such attacks take place when a bug, ex. corrupted file, enters the systems of a financial institution, from here, the bug encrypts the user's files, blocking the firm or the user from accessing them (Zenzero, 2024). The files are leaked in cases of data breaches and sold back to the firm in case of a ransomware attack. Institutions can adopt the Principle of least privilege to avoid such attacks however, these render useless to email attack vendors. Institutions have set up appropriate protocols to minimise the losses in such attacks (SentinelOne, 2024). AI can be used to detect irregular patterns and Deep learning (DL) AI, can use its neural decision-making properties to alter firewall configurations to further secure a firm's internal data and seamlessly follow the protocol. AI-infused cybersecurity models allow for a swift and pre-emptive response towards cyber-attacks, moreover, the strength of an AI can be tested with high-resilience simulations that train and ready the machine to combat all forms of cyber-attacks (Zenzero, 2024). AI is also an impactful tool if a firm is looking to reduce its operational costs. Automated protocol undertaking removes the need for human interference. Such a tool can enhance public trust and keep a bank out of troublesome news. This creates a welcoming environment for new clientele, allowing the bank to prosper, whilst reducing operational costs and losses to cybercrime. AI can also minimise human errors made, which lead to data leaks and other costly expenses.

Cost of data leak based on where AI is integrated into the security systems

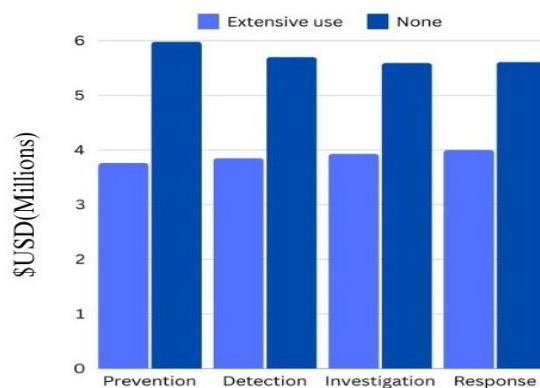


Figure 6. Illustrating the cost of data leak based on AI deployment. Illustrated by author, Source

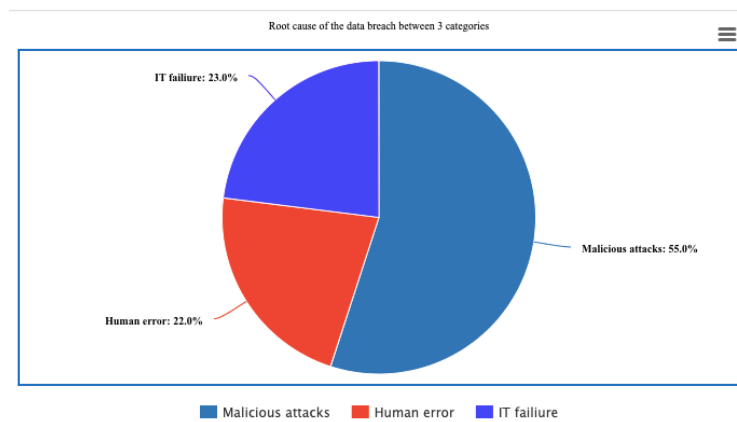


Figure 7. Illustrating the root causes of data leaks at financial institutions. Illustrated by author, Source

Lastly, AI has been at the forefront of developments in ATMs to improve their security profile. ATM theft is majorly focused around two types of attacks: Physical Burglary and Terminal-related fraud attacks. €173m in losses to terminal-related fraud attacks were reported in 2023, out of which €146m were due to card skimming (E.A.S.T, 2023). The federal Bureau of Investigation (FBI) suspected that Debit Card skimming grew by 96% in 2024 compared to previous years (FEDERAL BUREAU OF INVESTIGATION, n.d.). Card skimming works when fraudsters steal the information on a suspect's card by using Overlay skimmers or as of late Wireless skimmers. Both serve a similar purpose, however, only overlay skimmers are present on-site as they lay onto the card reader acting as a mask to hide the real one beneath. The stolen card information is either used directly to purchase goods online or is sold to interested buyers on the dark web. Banks have been attempting to tackle the issue of card skimming for years. Fraudsters only reveal a partial section of the 16-digit identification code making it tougher for banks to pinpoint the correct card. However, with the help of AI, banks have been enabled with the power to detect and flag potentially fraudulent transactions and develop a pattern of frequently visited online merchants to mitigate the losses of stolen cards. "The algorithm analyzes cards and merchants, generating links between them based on the associated risk." (ELYSE CUTTLER, 2024). Furthermore, AI has equipped banks with the capability to "predict the full 16-digit card numbers of these compromised cards" (ELYSE CUTTLER, 2024), helping them block the suspect's cards at a faster pace. Lastly, the final method of a terminal attack is called a Bank identification number (BIN) attack. In such attacks, fraudsters utilize the first 4-6 digits of a victim's card number (Ayush Rodrigues, 2024), and feed the numbers into an algorithm to generate a series of potential working cards. Attackers then use any working combinations to "bombard a card issuers system with transaction authorisation requests" (Alex Robinson, 2020). Such attacks can overwhelm a bank's operations team and reduce customer confidence. Previously mentioned anomaly detection can allow banks to flag suspicious activity and mitigate the risks of such attacks. AI can be incorporated into a Multi-layered defence strategy as the dynamic capabilities of AI that allow it to adapt in real-time are highly beneficial for financial institutions. (Alex Robinson, 2020). Lastly, AI can be greatly beneficial in completely disallowing any fraudulent cash withdrawals at ATMs with the use of biometric scanners. Biometric password protection has been widely adopted in recent times. The most popular form is facial recognition present in our mobile phones. Introduced in 2017, Apple's facial authentication system added a layer of impenetrable security to its devices. The tool creates a depth map of your face and stores the information in a remote part of your phone's internal motherboard. Apple's face ID has acted as a security feature to protect FinTech applications from potential intruders. A majority of the applications use the feature as the primary security layer guarding sensitive financial information. A 2021 report found that 38% of people rely upon Face ID as the main security feature on banking sites (iProov, 2021), with "30% of people doing *all* of their banking remotely on their mobile devices" (iProov, 2021). Similar technologies should be adopted by financial institutions to robust the security of their ATMs. This added layer of protection would make the withdrawal portal accessible to the specific owner of the card, via a biometric scan of their finger, retina, face, or voice. Voice recognition software has been implemented into the Call management systems (CMS) of several financial institutions globally. The tool works by analysing a segment of the user's voice (consented) and then breaking the voice into digital signals, this process is called Analogue-to-digital conversion (A/D) (Li et al., 2023). "The system then compares the signals to a database of known words and patterns to determine the intended command." (Alexander S. Gillis, n.d.). However, Voice assistants only act as a layer of security and cannot (as of today) be the frontal force in tackling financial fraud. The University of Waterloo conducted a test in which they bypassed voice recognition systems with a "99% success rate after only six tries." (Media Relations, 2023). The storage of each 'voice signature' onto a cloud-based system sparks several concerns over user privacy and further concerns with data encryption (Li et al., 2023). Biometric scans in ATMs need to be far more robust and reliable to be widely adopted. In 2019, Spanish 'CaixaBank' became the first multinational firm to adopt facial recognition into its ATMs as a biometric security layer. A study conducted by the bank highlighted that 70% of its users would be willing to swap a numerical pin for a biometric alternative (PRESS RELEASE CaixaBank Executive Communication and External Relations Division, n.d.). The facial recognition used by the bank utilizes 16.000 facial points to create a unique and detailed depth map of the user's face (VisionAI, 2021).

The system, built off Deep learning (DL) by Fujitsu Laboratories of America Inc. Facephi was built to understand facial expressions and use this understanding to build a more efficient biometric system.

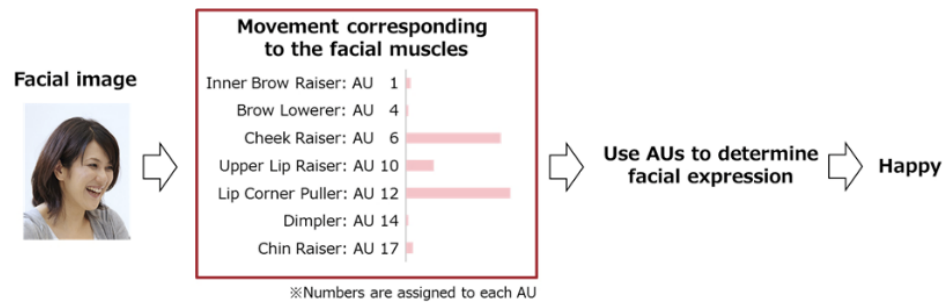


Figure 8. Illustrated flowchart of DL understanding of facial expressions. Illustrated by Source

Financial firms look to implement technologies that balance both user safety and maintain or improve efficiency. Facial recognition is a tedious tool that works seamlessly if the AI is well-trained on large data sets. A reliable facial recognition software must be usable in all feasible scenarios. The cost for research and development (R&D) for such industry-leading software lies high in the range of millions, however, this one-time price is far outweighed by the recurring cost of losses to bank fraud. Although Caixa Bank's venture into facial recognition was limited to 100 ATMs in Barcelona, the technology has the potential to be widely implemented globally.

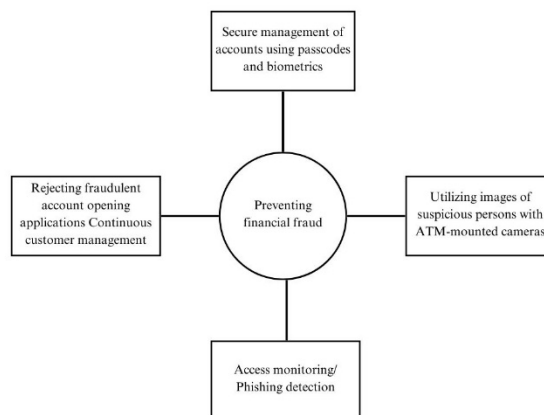


Figure 9. Illustrating key ways of preventing financial fraud at Sevenbank. Illustrated by Author, Source

- Sevenbank successfully rolled out 6000 Facial-recognition armed ATMs in September 2019
- Sevenbank has 27,000 ATMs in 47 prefectures in Japan (Bank, n.d.) with 20,000 supporting facial recognition (TAKAYUKI MAEDA, 2023).

Risks of Implementing AI Into Key Financial Infrastructure and Evolving Government Policy

AI has been at the forefront of technological developments at financial institutions globally. However, the implementation of AI comes with risks that are often overlooked whilst attempting to embrace the future. Most artificial intelligence relies on learning patterns in data and decoding the patterns to create a set of commands to undertake. Most data fed to DL and ML algorithms contains sensitive information, including behavioural patterns, biometric

information, and long-strain conversations. The data is crucial for the AI to function efficiently and reliably. Data sets vary in size, from small data sets starting at approx. 10,000 samples ((Hrvoje Smolic, 2024), larger data sets stretch over millions (dependent on task complexity). The data provided is encoded and the AI can only learn from what it is provided with. However, there are several issues with the growing volume of data being collected as people fear that a data leak may result in the exposure of the sensitive information of millions globally. 181 Zettabytes of data is estimated to be collected globally by the end of 2025 (Petroc Taylor, 2023), however 70% of consumers deem data collection as an “immoral practise” (Michael Behr, 2022). Given that data is the fuel for AI, concerns around privacy and bias are on the rise. AI could be vulnerable to hacking groups looking to leak user data or sell sensitive information on the dark web. There are several ways AI can be misled and hacked, causing it to automatically leak sensitive data that was part of its learning set. Chatbots (ex. ChatGPT) can be targeted numerous times, allowing the hacker to learn keywords that trigger the spill of sensitive data. This attack is called ‘Prompt injection’ and is an accessible way to uncover the data set an AI has been trained on (Kevin Poireault, 2023). Another attack, used by hackers is called ‘Data poisoning’, data poisoning occurs when an AI is fed “malicious or biased data into the training dataset to influence the behaviour of the trained model when it encounters similar data in the future” (Kevin Poireault, 2023). Such an attack could be catastrophic for financial institutions as they are rapidly embracing AI Chatbots. Simultaneously, consumer trust in such technologies is growing which in turn makes a corrupted chatbot a great liability for both the firm and the customer. It is crucial for Fintech firms to carefully monitor their system of AIs in case of an attack as these can be executed by anyone with no prior knowledge or high understanding of IT. Data poisoning can be done by a “disgruntled employee” (Swiss Re Institute, 2023) meaning maintaining a high level of security at data processing centers and adopting the principle of least privilege is crucial. However, it is important to remember that such an attack could be done by an individual with no “access to the computer network it runs on” (Shaun Waterman, 2022). Data poisoning can be damaging to financial infrastructure as it can trigger the AI to spit a pre-determined response which a hacker could use to its advantage, for ex. “an exceptionally high creditworthiness or insurance score” (Swiss Re Institute, 2023). Biased data can result in a biased AI service, which, as explored previously creates societal splits and worsens the image of Artificial intelligence whilst putting certain groups of people at a disadvantage. Lastly, hackers are utilising cloud storage to their advantage and hacking into remote servers to access extremely sensitive customer data. Servers holding the financial information of a bank's customers can be under the threat of hackers in early 2024, researchers claimed an open-source software named “Ray” used to scale AI models has left thousands of servers compromised. “Because distributed AI workloads require hundreds or thousands of processors to run, a single attack can result in the compromise of multiple machines” (Thomas Brewster, 2024) The leak of financial data can be greatly costly to both the financial institution and the victim of the attack. Such instances allow us to realize that the risks of AI have already become a reality, and our data is less safe than generally believed. By 2029, there will be just under 1 million servers running data processing and storage for AI models (Anton Shilov, 2024). This creates a huge vulnerability for consumers worldwide and acts as an opposing reality to the ease AI brings us. The leaking of sensitive biometric data can be used by hackers to impersonate the victim and take control of their digital presence. Such attacks have the possibility of going unnoticed by the authorities and could be a substantial risk for financial institutions. Occurrences as such have slowed the output of evolving government policies on the implementation of AI and have reduced its current potential.

Government Regulation on the Use of AI in the Financial Services Industry (FSI).

Country/Organisation	Abstract	Regulations in the FSI	Date released
----------------------	----------	------------------------	---------------

European Union (EU)	The EU released its AI act and created a tiering system to regulate the use of AI and keep consumers safe. The EU upheld its human-centric approach and ensured a high level of safety within crucial sectors ex. Health, finance, and law.	As of the 29th of August 2024, the EU outlines two use cases of AI in the Financial services industry as high risk. "AI systems used to evaluate the creditworthiness of a person, and for risk assessments and pricing for life and health insurances." (Benjamin Christopher Ilg, 2024). As to biometric data, 'emotion recognition systems' are completely prohibited whilst all other forms of Biometric data processing must be done under the highest level of restrictions within the EU. (Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) (Artificial Intelligence Act), 2024).	13 th June 2024
The United States of America (USA)	As of August 2024, The USA does not have a specified bill for the development and use of AI as well as any regulations. However, several state-specific laws have been altered to suit AI. A blueprint for a future bill brought forward in the Biden administration highlights 5 principles that must be followed. - Algorithmic bias protection - Data privacy - Safety and efficacy - Notice and explanation - Human Alternatives, consideration, and feedback.	The US treasury stated that it "supports responsible innovation and competition in the financial sector and seeks to promote a financial system that delivers inclusive and equitable access to financial services that meet the needs of consumers, businesses, and investors while maintaining stability and market integrity, protecting critical financial sector infrastructure, and combating illicit finance and national security threats."(Treasury Department, 2024). The treasury also acknowledges the growth of AI in the sector and will "continuing to monitor technological developments and their application and potential impacts in financial services" (Treasury Department, 2024). The Financial Stability Oversight Council (FSOC) noted the use of AI in the financial sector as a "vulnerability" (Financial Stability Oversight Council, n.d.) in a 2023 report. The treasury lists the risks of AI in the financial sector- "Potential risks associated with AI use for impacted entities may include bias, discrimination, monoculture, concentration, fraud, herding, hallucinations,	A Notice by the Treasury Department on 06/12/2024.

		explainability, conflicts, reputational risk, and data privacy risks, among others.” (Treasury Department, 2024).	
--	--	---	--

Peoples Republic of China (PRC)	The Chinese government's 'Provisions on Management of Generative Artificial Intelligence Services' has a detailed list of compliances that 'generative AI providers' must follow to provide their services. The regulatory bill highlights its interests in the growth of the technology and aims to "Promote a healthy development and regulated application of generative artificial intelligence, safeguard national security and social public interests, and protect the lawful rights and interests of citizens, legal persons, and other organizations." (Cyberspace Administration of China et al., 2023). The bill is clear on data privacy and outlines "Data labeling rules" (Cyberspace Administration of China et al., 2023) in which staff must be trained accordingly. Furthermore, there is an increased sense of understanding around bias and the bill enforces a provider to "prevent discrimination based on nationality, religion, country, region, gender, occupation and health in the design of the algorithm, training data set, model generation, optimization, and service provision" (Cyberspace Administration of China et al., 2023) "Article 21 of the AI Measures outlines the liability provisions for violations and non-compliance." (White&Case, 2024) According to Articles 253 and 291 of the Criminal Law of China, illegally obtaining personal data and spreading the data or utilising it for the development of ML algorithms can be an offence that can lead to up to seven years in prison. According to China's Personal Information Protection Law (PIPL), "failure to comply with the PIPL can result in penalties such as fines up to 50 million RMB, revenue confiscation and even business cessation." (White&Case, 2024)	The PRC has issued several guidelines on the use of AI in the financial services sector. The guidelines are written by the National Financial Standardization Technical Committee. The 'People Bank of China' acts as a regulatory board that oversees AI-integrated financial operations taking place within the country (People's Bank of China, China Banking and Insurance Regulatory Commission, n.d.). The regulations demand the AI provider to disclose Algorithm change information in mainly automated financial services as the adjustment of strategies is more frequent and rapid which may lead to "risky activities" (Guidance on information disclosure for financial applications based on artificial intelligence algorithms., 2023). The regulations ask the provider to explain the developed framework to the consumer and the safeguards in place in case of "Abnormal situations" (Guidance on information disclosure for financial applications based on artificial intelligence algorithms., 2023) and other uncontrollable factors. The providers are also commanded to disclose the effective data and detailed impact of changes to the AI algorithm. Alongside, the changes from the previous version and the reason for change. The service provider is tested under compliance audits for the financial application of artificial intelligence. This reduces technical and operational risks. The audit tests for Security, Explainability, Accuracy, and Performance ((Guidance on information disclosure for financial applications based on artificial intelligence algorithms., 2023).	July 13, 2023, enforced August 15, 2023.
---------------------------------	---	--	---

Sociocultural Stigmas Around the Implementation of AI Into the Financial Services Industry

AI has been implemented in several industries globally and government policies are adapting to allow for innovations to take their place in the work environment. AI, its reach, and its capabilities are growing rapidly. Industry professionals have started to question whether or not AI is fit to take their jobs. Automation of repetitive tasks like customer service, data analytics and prompt engineering can be completely replaced or greatly assisted by advanced AI models. 14% of the global workforce is said to be affected by AI by 2030 (GilPress & Statista, 2024), with 30% (300 million) jobs reported to have become completely automated globally (by 2030)(GilPress & Statista, 2024). Artificial intelligence thrives in mathematical environments, hence its adoption into the financial industry can be widespread. Therefore, having a substantial impact on job security within the sector. The growth of AI-enhanced tools in the FSI has been greatly funded. Financial institutions are banking on AI to “augment or automate” (Morgan Stanley, 2023) tasks to reduce their paid workforce and cut operating costs. As of 2023, a Nvidia survey analysed that AI automation had cut running costs for banks by approximately 10% (Nvidia, n.d.). Assuming, at the current rate of AI adoption, this percentage will grow significantly. However, this comes with social stigmas as companies are looking to maximise financial efficiency. As a result of this, 54% of jobs in the financial sector are under the risk of total automation, a majority of which are low-paying entry-level jobs (Citi Bank, 2024). This has had a great impact on job security in the industry. Furthermore, it could lead to stunted growth as industry professionals are hesitant to allow it to undertake full tasks on its own, in case the firm sides with the cost-effective automation. Aside from job security, it is important to monitor AI in this sensitive industry, as AI can be prone to bias (as analysed previously), and letting it undertake complete tasks, like creating reports is dangerous, as AI bots are prone to creating false-information and spewing made-up facts. Only 26% of institutions understand the risks and stigmas around AI (Nvidia, n.d.). Lastly, Artificial intelligence models require a great volume of resources to train. Chatbots, of the complexity financial institutions would prefer, require 700.000 litres of water to train, and a further 500ml for every conversation (ALAN MARTIN, 2023). Such chatbots emit 4.2g of Carbon dioxide per query and consume 3.6 to 36kJ of energy (Pilar Girvan, 2024). Such great volumes of required raw material and emissions in the age of greener thinking may put additional stress on financial institutions.

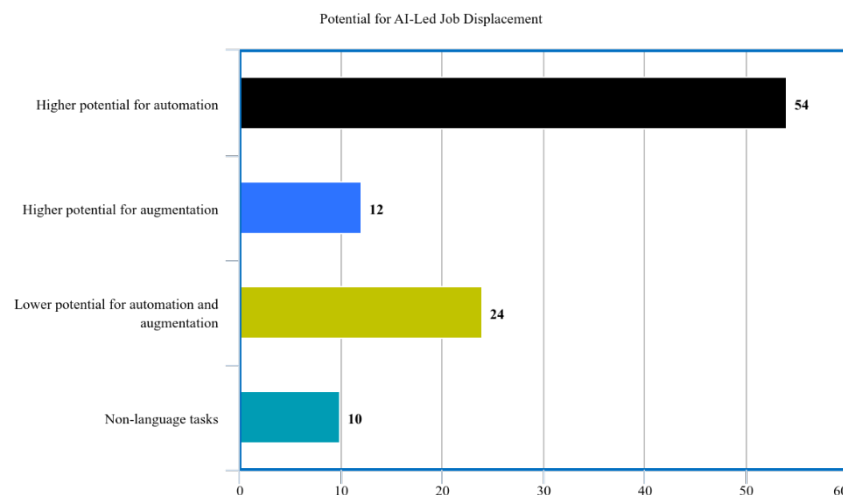


Figure 10. Potential AI Job displacement in the Banking sector. Illustrated by Author, Source

Conclusion

The exploration of AI's integration within the Financial Services Industry (FSI) reveals both promising advancements and significant challenges. The paper analyses how AI has become a central component in the industry's pursuit of efficiency and cost reduction, with numerous companies implementing these technologies to streamline operations. However, the analysis has also allowed us to understand a variety of challenges faced by AI providers globally. The insights suggests that while AI contributes to enhanced financial efficiency and improved customer experiences, it raises concerns about job security, environmental damage and societal acceptance. The ongoing rebuttal surrounding AI's role in the FSI reflects a broader tension between embracing innovation and addressing the ethical and cultural implications of its widespread adoption.

In conclusion, the current state of AI in the financial sector is characterized by a thin balance between innovation and regulation to ensure customer safety and data protection. As the industry continues to evolve, it will be essential for stakeholders to navigate these challenges thoughtfully, ensuring that the benefits of AI are realized without compromising societal values and customer trust. The paper emphasizes the need for ongoing research and dialogue to better understand and address the multifaceted impact of AI on the financial services landscape. I believe FinTech firms and instrumental financial institutions need to cooperate and work together to maximise the use of Artificial intelligence. AI can be a tool to enrich a worker's experience, rather than a replacement to a bank's human workforce. Governments, namely ones who have not yet set out clear regulations for the sole development and use of AI technologies, must do so to robust the safety of the data of their citizens whilst ensuring a level of clarity between industry and consumer. The trust of the general public is a necessity for a future in which AI is concreted into the financial services sector.

Acknowledgments

I would like to thank my advisor for the valuable insight provided to me on this topic.

References

- ALAN MARTIN. (2023). AI chatbots guzzle enormous amounts of water, study finds. *The Standard*.
<https://www.standard.co.uk/news/tech/ai-chatgpt-water-usage-environment-study-b1073866.html>
- Alex Robinson. (2020, November 6). *Can BIN Attacks Be Consigned to the Trash? -Video-*. Feature Space.
<https://www.featurespace.com/newsroom/stopping-bin-attacks/>
- Alexander S. Gillis. (n.d.). *Voice recognition*. TechTarget. Retrieved August 28, 2024, from
<https://www.techtarget.com/searchcustomerexperience/definition/voice-recognition-speaker-recognition>
- Anton Shilov. (2024). *AI becomes leading server workload as shipments of other servers drop*.
<https://www.tomshardware.com/tech-industry/artificial-intelligence/ai-becomes-leading-server-workload-as-shipments-of-other-servers-drop>
- Ayush Rodrigues. (2024, April 25). *WHAT IS A BIN ATTACK?* Checkout.Com.
<https://www.checkout.com/blog/what-is-a-bin-attack>
- Bank, S. (n.d.). *Integrated Report 2023*. <https://www.sevenbank.co.jp/english/ir/>
- Benjamin Christopher Ilg. (2024, June 19). *AI in finance*. European Commission.
https://finance.ec.europa.eu/news/ai-finance-2024-06-19_en
- Benjamin Stratton. (n.d.). *Fintech Market Growth Statistics*. Retrieved August 27, 2024, from
[https://bluetree.digital/fintech-market-growth-statistics/#:~:text=The%20fintech%20sector%2C%20which%20currently,reaching%20\\$1.5%20trillion%20by%202030.](https://bluetree.digital/fintech-market-growth-statistics/#:~:text=The%20fintech%20sector%2C%20which%20currently,reaching%20$1.5%20trillion%20by%202030.)

- Citi Bank. (2024). *AI in Finance*. www.citi.com/citigps.
- Cyberspace Administration of China, State Administration of Radio and Television, Ministry of Public Security of the People's Republic of China, Ministry of Industry and Information Technology of the People's Republic of China, Ministry of Science and Technology of the People's Republic of China, Ministry of Education of the People's Republic of China, & National Development and Reform Commission of the People's Republic of China. (2023). *Interim Measures for the Administration of Generative Artificial Intelligence Services*. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm
- E.A.S.T. (2023). *ATM Physical Attacks rise in Europe*. <https://www.association-secure-transactions.eu/atm-physical-attacks-rise-in-europe/#:~:text=This%20decrease%20was%20primarily%20due,is%20in%20the%20table%20below>.
- ELYSE CUTTLER. (2024, July 18). *Inside the algorithm: How gen AI and graph technology are cracking down on card sharks*. Mastercard. <https://www.mastercard.com/news/perspectives/2024/inside-the-algorithm-how-gen-ai-and-graph-technology-are-cracking-down-on-card-sharks/#:~:text=Using%20generative%20AI%2C%20advanced%20algorithms,than%20we%20previously%20thought%20possible>.
- FE DER A L B U R E A U O F I N V E S T I G A T I O N. (n.d.). www.ic3.gov
- Financial Stability Oversight Council. (n.d.).
- Fred Savage. (2023). *Chatbots: Vector Analysis, Competitor Leaderboard & Market Forecasts 2023-2028*. <https://www.juniperresearch.com/research/telecoms-connectivity/messaging/chatbots-trends-research-report/>
- GilPress, & Statista. (2024). *What Percent of Jobs Will Be Replaced by AI – Statistics 2024*. <https://whatsthebigdata.com/ai-replacing-jobs-statistics/>
- Giudici, P. (2018). Fintech Risk Management: A Research Challenge for Artificial Intelligence in Finance. *Frontiers in Artificial Intelligence, 1*. <https://doi.org/10.3389/frai.2018.00001>
- Glassdoor. (2024). *Customer Support Agent salaries in United States*. https://www.glassdoor.co.uk/Salaries/customer-support-agent-salary-SRCH_KO0,22.htm?countryRedirect=true
- Guidance on information disclosure for financial applications based on artificial intelligence algorithms., Finance industry standards of The People's Republic of China (2023). <https://hbba.sacinfo.org.cn/attachment/onlineRead/228bc5a5110054687f3acef5900fed4fae0fe4cce70507d252bf7cd755b05761>
- Han, Y., Chen, J., Dou, M., Wang, J., & Feng, K. (n.d.). *Academic Journal of Management and Social Sciences The Impact of Artificial Intelligence on the Financial Services Industry*.
- Hrvoje Smolic. (2024, April 10). *How Much Data Do You Need for Machine Learning*. Graphite Note. <https://graphite-note.com/how-much-data-is-needed-for-machine-learning/#:~:text=Examples%20of%20machine%20learning%20with%20small%20datasets,-According%20to%20a&text=More%20than%20half%20of%20the,that%20could%20diagnose%20skin%20cancer>.
- Human in the loop*. (n.d.).
- iProov. (2021, July 7). *How Many People Use Face Biometrics? (Biometric Statistics)*. IProov. <https://www.iproov.com/blog/face-biometric-statistics-stats>
- Jamie Verdi. (n.d.). *A brief history of the evolution of fraud technology*. Alloy. Retrieved August 29, 2024, from <https://www.alloy.com/blog/a-brief-history-of-the-evolution-of-fraud-technology>
- Jeffrey Dastin. (2018, October 11). *Amazon scraps secret AI recruiting tool that showed bias against women*. Reuters. <https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/>
- Jonty Bloom. (2024, February 1). *Could AI “trading bots” transform the world of investing?* <https://www.bbc.co.uk/news/business->

- 68092814#:~:text=Generative%20AI%20can%20also%20simply,information%20or%20completely%20fabricate%20facts.
- Kevin Poireault. (2023, June 27). *How Hackers are Targeting Large Language Models*. Infosecurity Europe. <https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/how-to-hack-large-language-models.html>
- Ksolves Team. (2023, November 2). *How is AI Reshaping ATM Cash Optimization?* Ksolves . <https://www.ksolves.com/blog/artificial-intelligence/how-is-ai-reshaping-atm-cash-optimization>
- laying down harmonised rules on artificial intelligence and amending Regulations (EC) (Artificial Intelligence Act)*. (2024). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&print=true1/171http://data.europa.eu/eli/reg/2024/1689/oj>
- Li, J., Chen, C., Rahimi Azghadi, M., Ghodosi, H., Pan, L., & Zhang, J. (2023). Security and privacy problems in voice assistant applications: A survey. *Computers and Security*, 134. <https://doi.org/10.1016/j.cose.2023.103448>
- List of acronyms 3 Management summary 4 Background 5*. (n.d.).
- Live Chat Benchmark Report 2024*. (n.d.).
- Media Relations. (2023, June 27). How secure are voice authentication systems really? *University of Waterloo*. <https://uwaterloo.ca/news/media/how-secure-are-voice-authentication-systems-really#:~:text=With%20some%20of%20the%20less,spoofing%20countermeasures%20are%20critically%20flawed.>
- Michael Behr. (2022). *70% of UK People Consider Data Collection 'Immoral.'* <https://www.digit.fyi/70-of-uk-people-consider-data-collection-immoral/>
- Morgan Stanley. (2023, November). How Generative AI Could Reshape Work. *Morgan Stanley*. <https://www.morganstanley.com/ideas/generative-ai-future-of-work>
- NatWest. (2023, November 6). *NatWest and IBM Collaborate on Generative AI Initiative to Enhance Customer Experience*. Natwest Group. <https://www.natwestgroup.com/news-and-insights/news-room/press-releases/innovation-and-partnerships/2023/nov/natwest-and-ibm-collaborateon-generative-ai-initiative-to-enhanc.html>
- OCBC Group. (n.d.). *OCBC Securities to triple young active investors with launch of Singapore's first AI stock-picker*. OCBC Group. Retrieved August 27, 2024, from <https://www.ocbc.com/group/media/release/2024/ocbc-securities-to-triple-young-active-investors-with-launch-of-singapore-first-ai-stock-picker#:~:text=This%20personalisation%20allows%20investors%20to,penchant%20for%20self%2Ddirected%20investing.>
- Oecd. (2023). *Using AI to support people with disability in the labour market*. <http://www.oecd.org/termsandconditions>.
- Pavlo Sidelov. (2021, April 21). *Anomaly Detection in Finance*. SDK.Finance. <https://sdk.finance/anomaly-detection-in-finance/#:~:text=Datasets%20used%20to%20train%20static,fail%20for%20this%20exact%20reason.>
- People's Bank of China, China Banking and Insurance Regulatory Commission*. (n.d.). https://www.gov.cn/gongbao/content/2018/content_5323101.htm
- Petroc Taylor. (2023). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025*. <https://www.statista.com/statistics/871513/worldwide-data-created/>
- Philip Olaseni Shoetan, & Babajide Tolulope Familoni. (2024). TRANSFORMING FINTECH FRAUD DETECTION WITH ADVANCED ARTIFICIAL INTELLIGENCE ALGORITHMS. *Finance & Accounting Research Journal*, 6(4), 602–625. <https://doi.org/10.51594/farj.v6i4.1036>
- Pilar Girvan. (2024, February 3). The Hidden Environmental Costs of Chat GPTs: A Conversation with Bing Copilot. *Bylines Scotland*. <https://bylines.scot/environment/environmental-costs-of-chat-gtps/>

- PRESS RELEASE CaixaBank Executive Communication and External Relations Division. (n.d.).
<https://www.caixabank.com/communication>
- Reddy Kunduru, A. (2023). *CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES ARTIFICIAL INTELLIGENCE ADVANTAGES IN CLOUD FINTECH APPLICATION SECURITY*. <https://cajmtcs.centralasianstudies.org>
- Sachs, G. (2021). *Working Conditions Survey*.
- SentinelOne. (2024, January 22). Cyber Security in Banking. Why Cyber Attacks on Financial Institutions are on the rise. *SentinelOne*. <https://www.sentinelone.com/blog/a-cyberwar-on-financial-institutions-why-banks-are-caught-in-the-crosshairs/>
- Shaun Waterman. (2022, March 1). Hacking Poses Risks for Artificial Intelligence. *AFCEA Signal Magazine*.
<https://cset.georgetown.edu/article/hacking-poses-risks-for-artificial-intelligence/>
- Sobolev, D. (2022). The Price of Happiness: Traders' Experiences of Work in Investment Banks. *Journal of Behavioral Finance*. <https://doi.org/10.1080/15427560.2022.2100385>
- Nvidia. (n.d.). *State of AI in Financial Services_ 2023 Trends*.
- Swiss Re Institute. (2023, June 14). *AI getting hacked – systemic vulnerabilities of a booming technology*. SONAR 2023, Swiss Re Institute. <https://www.swissre.com/institute/research/sonar/sonar2023/ai-hacked-vulnerabilities-booming-technology.html>
- TAKAYUKI MAEDA. (2023, May 25). *Seven Bank plans Japan's first facial recognition ATM service*. Nikkei Asia.
- Thomas Brewster. (2024, March 26). Hackers Breached Hundreds Of Companies' AI Servers, Researchers Say. *Forbes*. <https://www.forbes.com/sites/thomasbrewster/2024/03/26/hackers-breach-hundreds-of-ai-compute-servers-researchers-say/#:~:text=Hackers%20are%20exploiting%20a%20vulnerability,researchers%20claim%20are%20unprecedented%20attacks.&text=Hackers%20may%20have%20breached%20hundreds,models%2C%20cybersecurity%20researchers%20have%20warned.>
- Treasury Department. (2024). *Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector*. <https://www.federalregister.gov/documents/2024/06/12/2024-12336/request-for-information-on-uses-opportunities-and-risks-of-artificial-intelligence-in-the-financial#footnote-19-p50051>
- Vedapradha, R., & Ravi, H. (2018). Application of Artificial Intelligence in Investment Banks. *Review of Economic and Business Studies*, 11(2), 131–136. <https://doi.org/10.1515/rebs-2018-0078>
- Virtusa. (n.d.). *Smart ATM*. Virtusa. Retrieved August 27, 2024, from <https://www.virtusa.com/digital-themes/smart-atm#:~:text=Smart%20ATMs%20provide%20further%20value,into%20customer%20behavior%20and%20preferences.>
- VisionAI. (2021, July 13). *CaixaBank Replaces PIN Code with Face Recognition for ATM Withdrawals*. VisionAI. <https://visionify.ai/caixabank-face-recognition-for-atm-withdrawals/#:~:text=Accuracy%20with%2016000%20security%20points%3A&text=With%20such%20many%20identification%20points,process%20of%20transaction%20than%20before.>
- White&Case. (2024, May 13). AI Watch: Global regulatory tracker - China. *White&Case*.
<https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china>
- Yonah Welker. (2023). Generative AI holds great potential for those with disabilities - but it needs policy to shape it. *World Economic Forum, AI Governance Summit(EMERGING TECHNOLOGIES)*.
<https://www.weforum.org/agenda/2023/11/generative-ai-holds-potential-disabilities/>
- Zenzero. (2024, July 1). *The Role of AI in Defending Against Ransomware Attacks*. Zenzero.
<https://zenzero.co.uk/news/ai-against-ransomware>