Global Banks

Mythos-class era: Cybersecurity a bigger concern than credit risk

European Banks

Kian Abouhossein [AC]
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

Amit Ranjan
(44-20) 7134-4576
amit.x.ranjan@jpmorgan.com
J.P. Morgan Securities plc

Specialist Sales contact details:

Gigi Sparling - Specialist Sales - European Financials
(44-20) 7134-0355
ghislaine.sparling@jpmorgan.com

Cybersecurity in Banks is currently one of the biggest undiscounted risks not reflected in Bank valuations in our view, partly due to the limited disclosure available which leads to a lack of comparability between banks on their preparedness or lack thereof to deal with emerging cybersecurity risk (pre-event and post-event processes), driven by advanced AI capabilities such as Frontier Models. While there is significant regulatory focus on capital ratios, we believe looking at cybersecurity risk through the lens of the capital framework is not the best approach. In our view, there should be an increased focus on cybersecurity driven liquidity risk and this should be **tested through increased infrastructure resilience testing and through a deposit-run liquidity haircut test as we believe liquidity, not credit risk, could be the main trigger in a scenario of a potential banking crisis with social media likely to trigger unprecedented volatility in deposit flows as we witnessed at Credit Suisse**. In this changing environment, we are likely to see differentiation between players, based on: i.) **Geopolitics** - US players are likely at an advantage, having early access to the most sophisticated AI models, with the US being the epicenter of AI developments (e.g. Project Glasswing), followed by potentially China which also seems to be ahead of peers, while Rest of the World is likely at a disadvantage; ii.) **Size and interconnectedness** as G-SIB banks are likely to have early access to test out the latest developments compared to smaller banks. We also start to question whether, rather than focusing purely on earnings, we should look to assign a 1x higher multiple (i.e. lower implied CoE) for 'sticky' client deposit banks with material excess deposits, based on our view of their ability to manage through the next crisis scenario. We believe a degree of premium for US GSIBs (currently at avg. 12.5x P/E 2028E, BBG consensus) compared to their global counterparts (European Banks at 9x P/E 2028E and Japanese megabanks at 12x P/E 2028E) could be justified due to lower CoE as the market factors-in better cyber risk preparedness through higher absolute scalable tech spending and early access to latest frontier models.

Frontier models such as Mythos and GPT-5.5 significantly reduce the timeline for discovering previously unknown **"Zero-day" vulnerabilities** from months and years to hours. While these models highlight the exposure of all global banks to cyber risks, on a bottom-up basis the banks **more exposed in our view would be those with old and multiple legacy infrastructure patched together and with ongoing underinvestments** : i.) banks with legacy core banking systems which run on code that was written a few decades ago but do not show the necessary agility to fix identified vulnerabilities due to lack of resources or lack of infrsatructure protocols; ii.) banks where core banking systems are vendor provided and the vendor does not show the necessary agility to release patches for identified vulnerabilities; iii.) banks with mutiple legacy platforms, for example due to historical M&A, thus providing a bigger pool of potentially vulnerable points and iv.) banks which are not getting access to the latest developments in the field, leaving them potentially exposed to a "known threat" for a longer period of time than peers who have such access. As an external observer, it is difficult for us to differentiate between banks on this basis as: i) we do not have enough information around the IT main, back office infrastructure, middle office and external vendor reliance of individual banks and hence we look at IT spend as a barometer of banks

See page 12 for analyst certification and important disclosures, including non-US analyst disclosures.

which at least have the resources to stay ahead of the curve and also fix these vulnerabilities as they arise. Based on Table 1, Tech costs averaged c.17% of Global Banks operating expenses in 2025 and while the definition of tech spend varies between players, making like-for-like comparison difficult, it provides a starting point for engaging in discussions with bank managements. As technology is scalable, we also focus on absolute spend, with US large cap banks well positioned with higher absolute spend on Tech compared to their global peers, while European banks generally operate with lower absolute tech budgets and face a delay in access to some of the latest developments, as evident, for example, in their absence from the April announcement on Project Glasswing by Anthropic.

Overall, we believe tech spend as well as cybersecurity specifically should be a bigger topic of discussion for Bank investors and managements, with a focus on developing a bottom-up understanding of the infrastructure that banks have. JPMC Chairman and CEO Jamie Dimon in his 2025 annual shareholder letter highlighted Cyber risk as one of the larger risks still in front of us that are multi-year and unresolved, "*Cyber risk. I have to mention this because it remains one of our biggest risks, and this is probably true for many other major industries and corporations. AI will almost surely make this risk worse. We invest significantly to protect ourselves and stay vigilant*." Our current cost growth forecast of an average 1.8% p.a. over 2025-28E for European Banks could see upward pressure from increased need for tech investments; however, we would also expect cost savings from increased AI usage over time, thereby neutralising the impact to some extent. We also see the need for an increased pace of legislation to deal with cybersecurity issues as financial crime becomes increasingly sophisticated - not through bank regulatory capital or liquidity requirements, but back-testing of infrastructure and processes in the case of a cyber attack event.

We have previously discussed the impact of increased usage of digital money and the development of DeFi market as being the next frontier for Global Banks (see Global Banks: The Next Frontier: Future of Global Banking to be defined by Digital Money) and developments in the cybersecurity space are expected to impact the DeFi market as well. The increased use of Agentic AI in financial services is also bringing in new risks and further expanding the attack surface. While the possibility of using cold wallets offers a limited degree of protection, in an era of rapid developments in Quantum Computing, DeFi markets remain vulnerable to cyber attacks as well. However, the Ethereum Foundation indicates that, while quantum computers will eventually threaten the cryptography Ethereum uses today, it has a dedicated post-quantum research team, and a structured "Lean Ethereum" roadmap targeting 2029 for full post-quantum protection. Standards such as EIP-8141 for account signatures, quantum-resistant application layer Zero Knowledge proofs and lean consensus roadmap are part of the developments in some of the areas which Ethereum Foundation sees as vulnerable to quantum attack.

Ironically, while digital-first authentication is the trend, as cyberattacks become more sophisticated, especially those enabled by AI plus device compromise, there is a possibility that **banks may re-emphasize physical possession factors (hard tokens/security keys) because they are generally more resistant** to remote theft, phishing, and some forms of spoofing. However, if such a scenario does develop, **banks would need to do a balancing act between convenience for customers**, which is disrupted by the need to carry physical devices vs. the safety offered by such a move. We could potentially also **see scenarios where circuit breakers are increasingly deployed**, for example, to limit the chain reaction damage from a cybersecurity incident. We have seen banks in Singapore, for example, deploy cooling-off periods for selected digital bank transactions with the objective of providing a window to the impacted user to detect and report any suspicious activity relating to their account, such as adding a new transfer recipient. We also see the pace of roll-out of Agentic AI for external use by banks being slowed down as the growing attack surface provided by the agentic ecosystem with third-party linkages could lead to caution with frontier models

highlighting vulnerabilities.

Anthropic's Claude Mythos Preview (Mythos, released in April 2026) under controlled evaluation by various authorised agencies (such as AI Security Institute in the UK) has been reported to demonstrate significantly more advanced AI cyber capabilities than any other models. These evaluations have demonstrated that Mythos could autonomously discover and exploit vulnerabilities on exposed networks, executing multi-stage attacks, work that would typically take human professionals days to complete. Mythos is just one example of future AI capabilities, with other models such as GPT-5.5 also demonstrating similar levels of performance (see Figure 1) on cyber evaluations by agencies, and we would expect more sophisticated models to be developed over time, meaning banks and regulators would need to be dynamic in their approach to dealing with the evolving cybersecurity landscape. While projects like Glasswing also demonstrate the power of collaboration between firms and authorities to use these models to strengthen cyber defences, with restrictions on general availability of these models, we believe the speed at which vulnerabilities are discovered is increasing and the reaction time between the identification of vulnerabilities and their patching is getting compressed, which should continue to pose a challenge.

With an increase in **cybersecurity related incidents, we believe cyber insurance will become increasingly relevant for banks** to avoid situations like Jaguar Land Rover (JLR) which, based on press reports (Source: FT) had to shoulder the full bill from a damaging cyber attack in 2025 due to a lack of cyber insurance. Munich Re estimates that the global **cyber insurance market premium totaled nearly US$15bn in 2025 and Munich Re experts anticipate the global premium volume to expand to around US$28bn by 2030, representing an average annual global growth rate of 15% between 2020 and 2030.** We note that the Financial Services industry is amongst the biggest payers of cyber premiums globally and in an era of increased cybersecurity risk, we would expect regulators to be increasingly focused on cyber insurance protection availed by banks. In our view, regulators should also look to incorporate cyber risk insurance into the operational capital profile for banks to incentivise the purchase of appropriate protection through cyber insurance.

In our view, **the advancement of AI-led cyber threats means it would be difficult to make a system 100% safe with vulnerabilities in codes more easily exploitable**. However, cyber threats are "institutionalized" with measures such as ROI being used by cyberattackers to measure the potential return against the investment needed to execute a cyberattack, banks which make this ROI hurdle rate higher by making the necessary upfront investments would be better placed than peers. At the same time, the AI-led developments potentially lower the cost to carry out a sophisticated cyber attack for bad actors, and hence it **would be interesting to see where the 2 curves of AI-led enhancements through patching of vulnerabilities and the ease of carrying out AI-led attacks intersect in the future.**

Kian Abouhossein [AC]
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

J.P.Morgan

Step up in cyber performance in frontier models increases cybersecurity risks for Banks...

Frontier models are the most advanced AI models available at a given moment, trained on massive datasets to deliver state-of-the-art performance across many tasks, representing the leading edge of AI capability. They typically power advanced reasoning, image and text generation, and agentic workflows. (source: Nvidia) Both Mythos Preview and GPT-5.5 are examples of Frontier Models.

Anthropic's Claude Mythos Preview, disclosed in April 2026 is such a Frontier Model which according to the the company revealed the fact that "*AI models have reached a level of coding capability where they can surpass all but the most skilled humans at finding and exploiting software vulnerabilities*." Anthropic also announced Project Glasswing, which it said was a new initiative that brings together Amazon Web Services, Anthropic, Apple, Broadcom, Cisco, CrowdStrike, Google, JPMorganChase, the Linux Foundation, Microsoft, NVIDIA, and Palo Alto Networks in an effort to secure the world's most critical software.

How is Mythos more advanced than tools previously available? In simple terms, 1. Speed of discovering and subsequently exploiting vulnerabilities is much faster for Mythos than previous tools; 2. Minor vulnerabilities can be exploited by combining into serious attacks. Again, the speed of attack by Mythos is much faster than previous tools; and 3. Mythos can reverse engineer exploits on closed-source software, and turn known but not yet widely patched vulnerabilities into exploits.

The AI Security Institute (AISI) in the UK conducted evaluations of Anthropic's Claude Mythos Preview (announced on 7th April) to assess its cybersecurity capabilities and confirmed a significant increase in capability, with the system able to autonomously find and exploit vulnerabilities, execute multi-stage attack chains end to end, and achieved a 73% success rate on expert-level hacking tasks which no model could complete before April 2025. The results from an early checkpoint of GPT-5.5 conducted by the Institute indicate that the GPT-5.5 model also reaches a similar level of performance on AISI's cyber evaluations, which suggests that this step up in cyber performance is a broader trend rather than being limited to one model alone.

The step up in cyber performance, while done in a controlled setup without taking into account potential defense mechanisms/security protocols in a real world environment, highlights the need for financial institutions to improve their cybersecurity defense setup.

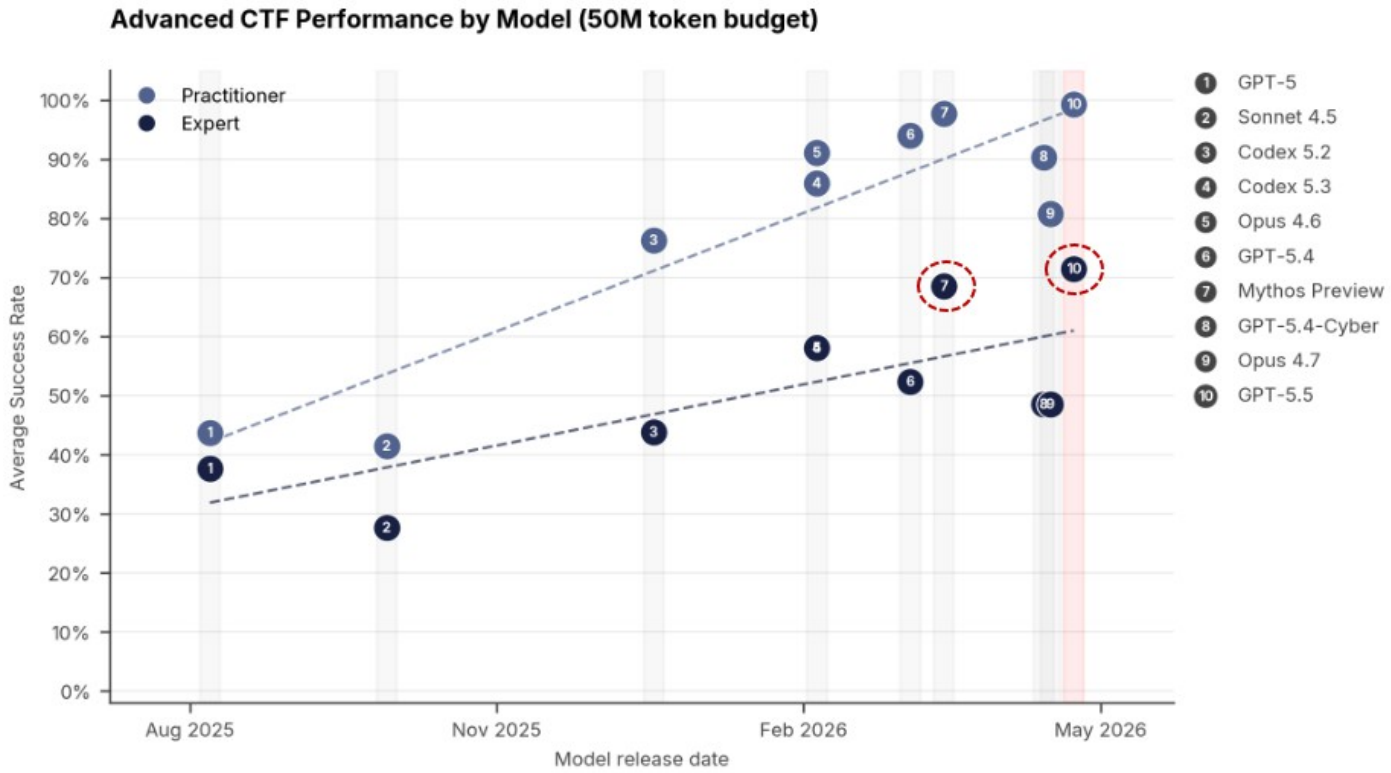
The threat is becoming increasingly real, with **Google in May 2026** indicating that for the first time, GTIG (Google Threat Intelligence Group) had **identified a threat actor using a zero-day exploit that it believes was developed with AI**. The criminal threat actor planned to use it in a mass exploitation event, but proactive counter discovery may have prevented its use.

In February 2026, AISI internally estimated that the **length of cyber tasks AI models could complete had doubled every 4.7 months since late 2024** – already an acceleration from their **November 2025 estimate of 8 months**. Since then, AISI reported on two new models, **Claude Mythos Preview and GPT-5.5, which substantially exceeded both doubling rate trends**. AISI in May said that it is unclear whether this represents a new, faster trend.

Kian Abouhossein [AC]
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

Figure 1: Step up in cyber performance over previous frontier models with Mythos and GPT-5.5

Average success rate on advanced cyber tasks at a 50M token budget. 27 Practitioner tasks, 21 Expert tasks



In CTF (capture-the-flag) challenges, AI models must identify and exploit weaknesses in target systems to retrieve hidden "flags".
Source: The AI Security Institute, UK (see here)

Anthropic has also noted that the number of vulnerabilities it has disclosed is a subset of the total number of vulnerabilities that Mythos Preview has found, since the process of independent human triage and review is the rate limiting step.

Figure 2: Anthropic dashboard of open-source vulnerabilities, showing vulnerabilities of all severities (rather than only those estimated high- or critical-severity by Mythos Preview).



Source: Anthropic

Kian Abouhossein [AC]
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

J.P.Morgan

...with different layers of banking infrastructure impacted by the threat of AI-led cyber attacks

Legacy core banking systems are the most vulnerable to this emerging threat from AI-led cyber attacks, as a portion of Banking platforms of Global banks still run on code which was written decades ago in languages such as COBOL and the current generation of coders may not be as familiar with the logic and comprehension of these codes written by their original coders. Frontier models such as Mythos are able to comprehend these code lines, enabling them to highlight potential vulnerabilities which until now were likely not detectable due to a lack of full comprehension.

Open Source Vulnerabilities can be particularly critical for banks' customer-facing platforms, and the widespread usage across banks of such open source libraries means a vulnerability could have material consequences if exploited by bad actors. Anthropic noted that *One example of an open-source vulnerability that Mythos Preview detected was in wolfSSL, an open-source cryptography library that's known for its security and is used by billions of devices worldwide. Mythos Preview constructed an exploit that would let an attacker forge certificates that would (for instance) allow them to host a fake website for a bank or email provider. The website would look perfectly legitimate to an end user, despite being controlled by the attacker.* wolfSSL indicates that over 5 billion applications and devices are secured with wolfSSL products, which in our view highlights the scope for potential disruption from exploitation of a vulnerability. In a May 2026 release, Anthropic indicated that it had used Mythos Preview to scan more than 1,000 open-source projects, which collectively underpin much of the internet, and that Mythos Preview had found what it estimates are 6,202 high- or critical-severity vulnerabilities in these projects (out of 23,019 in total, including those it estimates as medium- or low-severity).

Vendor firmware from third-parties is often used by banks and a delay or too long a patch cycle in firmware which cannot be remotely patched would expose the banks to cybersecurity risks. The G7 group of countries note that AI software supply chain security is becoming increasingly important, with several international initiatives underway. As one component of this effort, the Group published actionable guidelines for public and private sector stakeholders on what is reasonable to expect in a Software Bill of Materials (SBOM) for AI, to improve transparency and cybersecurity along the AI supply chain. It consists of a structured record, or inventory, of details and supply chain relationships for the various components used in building an AI system.

Concentrated dependency on cloud providers is another potential vulnerability, with the FCA noting that if multiple financial institutions all rely on one AI platform (a concentration risk) and that platform has a vulnerability, an AI-augmented attack could simultaneously hit many targets, potentially threatening financial stability. Without new approaches, traditional cyber defences and investigatory methods could be outpaced by self-evolving AI threats.

Kian Abouhossein [AC]
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

J.P.Morgan

US large cap banks better positioned, with US being the center of latest AI developments followed by China

We see shifting geopolitics playing a role in AI dominance as the U.S. takes the lead, being the center of major AI developments/breakthroughs, followed by China which also seems to have advanced its own models and strategy around AI. Europe seems to be at a disadvantage currently, as also reflected in the recent ban on some Anthropic models by the US government, which, citing national security authorities, has issued an export control directive to suspend all access to Fable 5 and Mythos 5 by any foreign national, whether inside or outside the United States, including foreign national Anthropic employees. Anthropic indicated that the net effect of this order is that it must disable Fable 5 and Mythos 5 for all customers to ensure compliance. Access to all other Anthropic models will not be affected. (source: Anthropic) Subsequently, we note press reports (source: Bloomberg) indicating that Anthropic in a statement on 27th June noted some lifting of restrictions: "*We received notice from the US government that Mythos 5, our strongest cybersecurity model, can be redeployed to a small group of cyber defenders and infrastructure providers*," Anthropic said in a statement. "*We are working to provision the approved set of providers and restore their access to Mythos 5 as quickly as possible. We are pleased to see this progress and continue to work with the government to expand access to Mythos 5 and make Fable 5 available for general use again*."

In the U.S., we would also note increased focus around **Quantum Innovation**, as reflected in the recent Executive Order (from June 22) on U.S. innovation in quantum technologies and strengthening national security in this area. We note that the order directs the relevant agencies and authorities to identify the national security implications of the increasing scale and performance of commercial quantum computers, such as the implications for the migration to **post-quantum cryptography**. In **Europe**, the European Commission in July 2025 adopted a **Quantum Strategy** to position Europe as a global leader in quantum by 2030. At the time, it acknowledged that despite its remarkable progress in quantum technology, the EU was lagging behind in translating its innovation capabilities and future potential into real market opportunities, while also struggling with fragmentation of strategies and roadmaps across Member States. In the **UK**, the **National Quantum Strategy** was published in March 2023, setting out a 10-year vision to be a leading quantum-enabled economy by 2033 and a plan for quantum technologies in the UK.

Overall, a scenario of early access to the latest models and developments in Quantum computing puts US banks at a likely advantage compared to their global peers when it comes to cybersecurity. In addition, U.S. banks with higher tech spending are also better positioned to invest and keep up with the latest developments in AI/cybersecurity in our view.

We note recent developments in Japan where the country's three megabanks are said to have gained access to Google LLC's new artificial intelligence (AI) model with high capability to detect vulnerabilities in computer systems according to press reports citing Japanese Finance Minister Satsuki Katayama (source: Kyodo News). In our view, this reflects the increased importance being placed by governments around the world on the threat from more sophisticated actors in financial cyber crime.

Kian Abouhossein AC
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

J.P.Morgan

Table 1: IT expenditure across a selection of Global Banks - US IT spend is the highest but Global Banks are catching up

Regional averages represent the average of the selected banks shown.

Company	2025 Operating costs ($bn)	o.w. IT expenditure* ($bn)	IT expenditure as % of costs
Amazon	636.9	108.5	17%
Alphabet	273.8	61.1	22%
JPM	95.6	18.0	19%
Bank of America	69.7	13.0	19%
Citi	52.9	12.2	23%
Morgan Stanley	48.3	7.1	15%
Goldman Sachs	37.5	6.0	16%
Bank of New York	12.9	4.0	31%
US Banks average		**10.0**	**20%**
Itau Unibanco	7.6	1.1	14%
Banco Bradesco	9.2	0.9	9%
Santander Brasil	4.7	0.7	14%
Banco do Brasil	7.0	0.4	6%
LatAm Banks average		**0.7**	**11%**
HSBC	33.5	7.4	22%
BNP Paribas	36.0	7.2	20%
Societe Generale	19.4	4.9	25%
UBS	36.5	4.8	13%
Barclays	22.9	4.6	20%
Deutsche Bank	23.4	4.0	17%
Lloyds	12.9	2.9	22%
ING	13.9	2.8	20%
CASA	17.4	2.6	15%
BBVA	16.2	2.3	14%
UniCredit	12.4	2.3	18%
Natwest Group	10.7	2.0	18%
CaixaBank	6.9	1.9	28%
Commerzbank	7.8	1.8	23%
Nordea	6.0	1.2	20%
ABN AMRO	6.2	1.2	19%
DNB	3.3	0.6	19%
Sabadell	2.9	0.3	10%
BAWAG	0.9	0.2	26%
European Banks average		**2.9**	**19%**
Industrial & Commercial Bank of China	34.4	4.0	12%
China Construction Bank	31.6	3.7	12%
Agricultural Bank of China	38.3	3.6	9%
Bank of China	35.7	3.5	10%
Mitsubishi UFJ Group	21.0	2.0	10%
Sumimoto Mitsui Financial Group	16.0	1.7	11%
DBS	7.1	1.3	19%
United Overseas Bank	4.7	0.9	18%
Asian Banks average		**2.6**	**12%**
Standard Bank	6.1	0.8	13%
First Abu Dhabi Bank	2.2	0.5	22%
Qatar National Bank	2.9	0.3	12%
MENA & Africa Banks average		**0.5**	**15%**
Westpac Banking Corp	7.5	2.0	27%
Commonwealth Bank of Australia	8.3	1.5	19%
ANZ Group	7.6	1.4	19%
National Australia Bank	6.4	1.4	21%
Macquarie Group	8.2	0.8	10%
Australian Banks average		**1.4**	**19%**

Source: J.P. Morgan estimates, Company data. Notes: The definition of IT expenses may not be comparable across companies. For Google/Alphabet AR25 - R&D costs and Amazon AR25 - Technology and Infrastructure expenses. For CASA, IT costs JPMe based on 1H24 share of IT investments. For JPM, IT expenditure based on growth disclosed in Company Update Feb'26. For BNP, we assume IT costs are 20% of total costs. For UBS and MS, Technology costs estimated at ~10% of Revenues. For DBK and ABN, IT costs from respective AR25. JPMe for GS, CBK, BAWAG, ING, SG, UCG. For BNY, tech investments disclosed in company call. For SAB, IT + Communications costs in AR25. For BAWAG, operating expenses according to consolidated P&L in AR25. HSBC: Based on 2023 disclosures. BARC: Based on 2023 disclosures of UK Tech/operations costs. LLOY: JPMe based on £3bn over 3Y, mostly in tech/data, 50% of Other expenses (proportion in line with history). NatWest: JPMe based on £3.5bn investment over 2023-25, 80% goes into tech/ data + 20% of admin costs. Australian Banks' reporting periods might not coincide with others. Japanese banks and Citi are based on 2024 data.

Kian Abouhossein [AC]
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

J.P.Morgan

Table 2: Excerpt of Comments by a sample of Global Banks on Mythos

		Date and Source
BNP	BNP Paribas SA is working with French artificial intelligence startup Mistral AI and other partners to prepare for cybersecurity threats posed by new models such as Anthropic PBC's Mythos.	Bloomberg - 26 May
STAN	Mythos can best be interpreted as a signal, in a much broader trend around sort of the curve on vulnerabilities. And so the bank has a sort of a two-part response. The first part is very operational in orientation. We have vulnerability management practices. We have software development practices. We have a defense in-depth set of controls implemented in the bank. And so we continue to tune those and advance those. And both our software development organization and our architecture and cybersecurity organization have been on top of this trend since long ago. And so Mythos is a point in time on a curve, but the trend has existed for quite some time. And so we have really been putting our energy into shifting left across the capability curve. So software and how AI is used inside the software development life cycle, as I mentioned earlier, to help our software developers, sort of identify, predict, determine where they might need to resolve something before it goes out the door. From a more strategic standpoint, vulnerabilities take advantage of complexity. They take advantage of technical debt, legacy, architecture, et cetera. And so you heard us talk today about our technology and really our bank game plan, which is to resolve the questions about technology lifecycle funding and obsolescence, and really take that estate to the next level of modernization. That is as large a defense against vulnerabilities and -- as anything else. And so, our cybersecurity, perimeter defenses, our threat intelligence is really quite strong. We have a defense in depth strategy. We're shifting left. And then, from a technology standpoint overall, the strategy helps by eliminating complexity and legacy technical debt. Very clear targets on reducing our third-party suppliers. So, this idea is how do we contain that estate in a way that we can mitigate against the risks better. The third-party ecosystem obviously not under immediate and direct control by Standard Chartered, right? And so, advancing our third-party security assessments in partnership with Tanuj's organization, who has procurement and relationship management for us with third-parties, has been an integral part of the last year. And we're well-served by it now in my view.	Investor Day - 19 May 2026
KBC	Cyber risk has become one of the main threats during the past few years, not just for the financial sector, but for the economy as a whole. This is partly driven by geopolitical tensions (state-sponsored cyberattacks), but is also increasingly supported by new technologies, such as the recent developments surrounding Anthropic's Mythos which enables AI-driven vulnerability discovery. Despite the limited information available about the Mythos threat, KBC has already taken necessary actions to increase vigilance and capacity to process a certain upcoming increase of zero day vulnerabilities.	1Q 26 Press release - 12 May
SEB	When it comes to Mythos, this is a development that of course has triggered a lot of conversations in many industries. Banking, no difference. And we are very active working with our suppliers. Many of our technological partners are part of the project Glasswing, which do have access to the Mythos model. So our way to work with our own exposures will be very much working with those partners. A second thing which we are certainly focusing in on progressing more broadly, is the ability to just reduce the cadence of releasing patches. So when there are vulnerabilities identified, the ability to quickly move forward, identify them and release patches that will continue to work with in parallel. But this is a development that we're following very closely and we are in close conversations both with authorities and our technology partners.	1Q 26 Earnings Call - 29 April
Bankinter	Mythos does not represent a fundamentally new category of risk rather an acceleration of existing cyber threats through AI automation. So what really changes is the speed, not the nature of the attack. So the point here is in order to react, it's just basically with the same tools trying to be much more agile and much more quick in the execution of the responses. So basically, the bank, ourselves or other banks what they need to do is to move faster in the responses, so from manual responses to automated responses, behavior-based defense to integrate AI into security operations, of course maintain human side. But basically this is the type of reaction. And I think also the type of reaction is not just a bank on bank individual type of reaction. I think this topic needs to be faced in a much more global approach in approach of an industry, of a country, of entire Europe. Because all these threats is not just a threat to the banks, it's just to the whole economy. So basically, this AI threat just changed the tempo of the cyber risk, not these fundamentals. And the right response is just basically to make sure that there is a coordinated, automated defense from all the industries and countries and basically reinforce the resilience. So the tool may be a new tool for the attackers, but it's also a new tool for the defenders. So I'm sure that everybody will accelerate the use of this new technology to accelerate the execution of the defense.	1Q 26 Earnings Call - 23 April
MS	We're working with Claude Mythos, the beta version and we are looking at different places inside of infrastructure where we will just continue to -- there'll just be continuous improvement. And that's going to go on with the firms that have the history that we have of cybersecurity infrastructure as the number one priority. This is not a new phenomenon. Cyber resiliency, as you know, has been a top priority at this firm and other firms. And yes, we are permissioned on Claude Mythos Preview. And certainly the reality is that cyber risk is in the ecosystem, as you know, an increasing threat broadly. And so our ability to, along with others, I assume, continue to act as a stalwart defense in our industry is important. So we will, I would imagine, collectively get better via that and then there will be other competitive products. This is another step in kind of the long tail technology transformation that we've been talking about that is once in a generation and now it's here. And as you've heard others say, cyber resiliency is a top priority at institutions like ours across all of our businesses. And if the ecosystem risk is likely increasing because of the quality and muscularity of the model, then we too need to get our gloves up and take it to another level. And that's exactly what you'd expect and we very much intend to do so. But I want to say on the back end that a lot of the good that AI is going to bring, both as an efficiency and effectiveness matter should not get dismissed because that's an important phenomenon that's going to continue to transform this firm.	1Q 26 Earnings Call - 15 April
GS	Cybersecurity has long been at the core of our business. And we have for a very, very long time put enormous resources forward to think constantly about cyber security risks in our business and it's something we've invested significantly in and continue to invest in. And as it's been widely reported, the large bank CEOs happen to be in Washington for a regular meeting of the Financial Services Forum. And so we were asked to come over to Treasury. By the way, it is not the first meeting that that group has gone over to Treasury to talk about cybersecurity risks over a number of years. So my first point is this is something the industry's focused on, it's something we're focused on, and there's nothing new in that focus. Obviously, the LLMs are making rapid progress and we're hyper-aware of the enhanced capabilities of these new models. With the help of the U.S. government and the model publishers, we are very focused on supplementing our cyber and infrastructure resilience. And this is part of our ongoing capabilities that we have been investing in and are accelerating our investment in. We're aware of Mythos and its capabilities, we have the model, we're working closely with Anthropic and all of our security vendors to kind of harness frontier capabilities wherever it is possible. And this will continue to be an important focus, but it's not new that as technology evolves, we have to continue to upgrade for cyber risk and make sure we're at the forefront of that.	1Q 26 Earnings Call - 13 April

Source: Bloomberg Finance L.P.

Kian Abouhossein AC
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

J.P.Morgan

Regulators have stepped up efforts to address the increased threat level

Regulators and governments across the globe have stepped up efforts to address the increased cybersecurity risks posed by Frontier Models. The **ECB's Digital Operational Resilience Act** (DORA) came into force in 2025 and ensures that banks, insurance companies, investment firms and other financial entities can withstand, respond to, and recover from ICT (Information and Communication Technology) disruptions, such as cyberattacks or system failures. DORA brings harmonisation to rules relating to operational resilience for the financial sector, applicable to 20 different types of financial entities and ICT third-party service providers.

DORA also aims to enhance the oversight of critical third-party providers, such as cloud service providers. In addition, DORA gave supervisors the task of testing (Threat-led penetration testing (TLPT)) whether a financial institution can detect, respond to, and recover from sophisticated attacks that mirror real-world threats, thereby providing a more systemic and enforceable framework for resilience. (Source: speech by Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, June 2026)

In 2024, the ECB conducted a cyber resilience stress test on 109 banks, 28 of which underwent a more thorough assessment of their ability to respond to, and recover from, a severe but plausible cybersecurity incident. The exercise was predominantly qualitative. Insights gained during the exercise were to be used for the wider 2024 Supervisory Review and Evaluation Process (SREP). At the conclusion of the exercise, the banks received a bank-specific report with recommendations for their improvement, which was to be followed up by the Joint Supervisory Teams as part of their regular supervisory activities. As this was not a stress test exercise focused on banks' capital, its results did not have an impact on banks' Pillar 2 Guidance.

Frank Elderson, Vice-Chair of the Supervisory Board of the ECB and Member of the Executive Board of the ECB, in a May interview, while acknowledging the lack of access to Mythos for European Banks stressed that *Banks need to redouble their efforts to identify vulnerabilities, even minor ones, using existing AI tools. And their approach to patching needs to be changed. Vulnerabilities once thought minor – and therefore typically only patched in longer cycles – need to be treated as urgent and must be fixed right away.*

In the US, an **executive order was signed in June 2026 by the President**, including the formation of an *AI cybersecurity clearinghouse, in voluntary collaboration with the AI industry and operators of critical infrastructure, that coordinates and deconflicts scanning for software vulnerabilities, discovers and validates such vulnerabilities, and coordinates and prioritizes remediation and distribution of vulnerability patches*. The order also addresses the topic of secure frontier model deployment with a call to **AI developers to provide access to "covered frontier models" to the Federal Government for a period of up to 30 days before they plan to release such models to other trusted partners**.

In the UK, **BoE** has indicated that in addition to global co-operation, it continues to work closely with the AI Security Institute to better understand potential financial stability risks involving frontier AI agents, as well as with the Digital Regulation Cooperation Forum (DRCF).

Kian Abouhossein [AC]
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

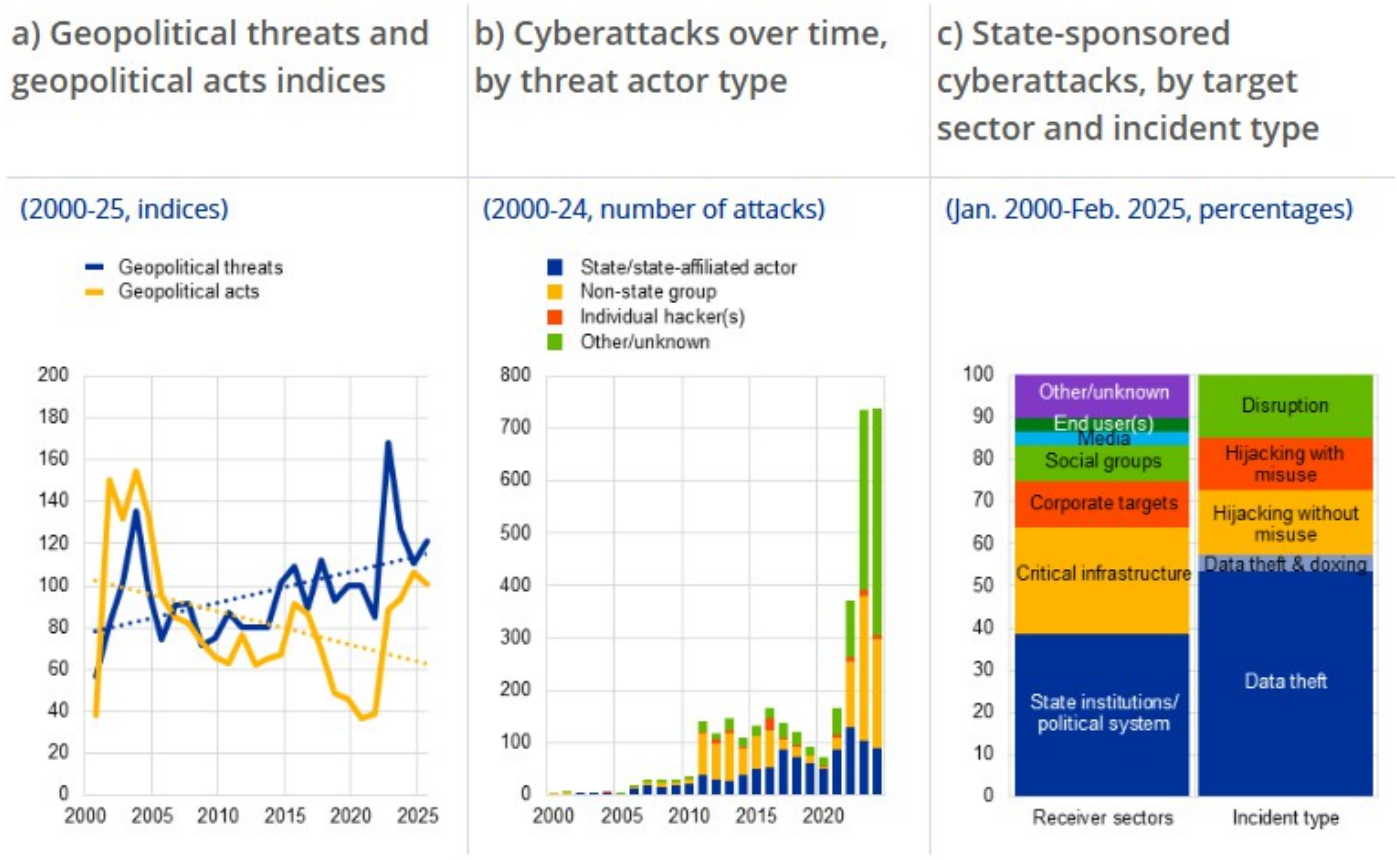
J.P.Morgan

Cybersecurity is an ever-growing threat with geopolitical reasons commanding a high share of attacks

In the current complex geopolitical landscape, the threat of cyberattacks from states and state-sponsored actors creates further need for Banks and other institutions to raise their guard as the attacks are likely to get more sophisticated.

ECB as part of its May 2025 Financial Stability Review (see here), noted that cyberattacks are playing an increasingly important role in the perpetration of hybrid conflicts. ECB noted that while the precise number of cyberattacks – both successful and unsuccessful – remains unknown, publicly disclosed data indicate that the volume of such attacks has increased substantially over the past decade, with a significant number of state-sponsored attacks seen in some years. Moreover, a number of countries conduct cyber activity not just via dedicated military or intelligence units but also via groups of cyber criminals acting on their behalf.

Figure 3: Geopolitical tensions are increasingly accompanied by state-sponsored cyberattacks



Notes: Panel a: the chart shows annual averages for the monthly geopolitical threats and acts indices. For 2025 the average covers January to April. Panel b and c: "State/ attacks conducted by nation-state actors or non-state actors for whom a state affiliation is suggested. They are the same attacks as those labelled "state-sponsored cyberat the annual numbers of cyberattacks up until 2024, while panel c only shows the subset of state-sponsored cyberattacks, but for the full sample period of the EuRepoC data 25 February 2025.
Source: ECB Financial Stability Review, May 2025



Kian Abouhossein AC
(44-20) 7134-4575
kian.abouhossein@jpmorgan.com

J.P.Morgan

Analyst Certification: The Research Analyst(s) denoted by an "AC" on the cover of this report certifies (or, where multiple Research Analysts are primarily responsible for this report, the Research Analyst denoted by an "AC" on the cover or within the document individually certifies, with respect to each security or issuer that the Research Analyst covers in this research) that: (1) all of the views expressed in this report accurately reflect the Research Analyst's personal views about any and all of the subject securities or issuers; and (2) no part of any of the Research Analyst's compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the Research Analyst(s) in this report. For all Korea-based Research Analysts listed on the front cover, if applicable, they also certify, as per KOFIA requirements, that the Research Analyst's analysis was made in good faith and that the views reflect the Research Analyst's own opinion, without undue influence or intervention.

All authors named within this report are Research Analysts who produce independent research unless otherwise specified. In Europe, Sector Specialists (Sales and Trading) may be shown on this report as contacts but are not authors of the report or part of the Research Department.

Important Disclosures

https://www.jpmm.com/research/disclosures, calling 1-800-477-0406, or e-mailing

the certifying Research Analyst's coverage universe can be found on J.P. Morgan's Research website,
country market index, not to those Research Analysts' coverage universe. If it does not appear in the Important Disclosu
India) and U.K. small- and mid-cap Equity Research, each stock's expected total return is compared to the expected tot
Research Analyst's, or the Research Analyst's team's, coverage universe of the relevant duration of the region. In our A
put no price target; in these cases, we expect the stock will outperform\perform in line\underperform the average total re
price target, no longer should be relied upon. An NR designation is not a recommendation or a rating. Some stocks may
because of either a lack of sufficient fundamental basis or for legal, regulatory or policy reasons. The previous rating s
team's, coverage universe. NR is Not Rated. In this case, J.P. Morgan has removed the rating and, if applicable, the price
this report, we expect this stock will underperform the average total return of the stocks in the Research Analyst's, or the
Research Analyst's, or the Research Analyst's team's, coverage universe): and Underweight (over the duration of the pri
the duration of the price target indicated in this report, we expect this stock will perform in line with the average to
outperform the average total return of the stocks in the Research Analyst's, or the Research Analyst's team's, coverage u
J.P. Morgan uses the following rating system: Overweight (over the duration of the price target indicated in this report, J

Coverage Universe: Abouhossein, Kian: Banco Sabadell (SABE.MC), Barclays (BARC.L), Commerzbank (DBKGn.DE), Goldman Sachs (GS), HSBC Holdings plc (HSBA.L), Morgan Stanley (MS), Santander (SAN.MC), Standard Chartered (STAN.L), UBS (UBSG.S)

Explanation of Equity Research Ratings, Designations and Analyst(s) Coverage Universe:

J.P. Morgan Equity Research Ratings Distribution, as of April 04, 2026

Company-Specific Disclosures: J.P. Morgan does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that the firm may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decision. Important disclosures, including price charts and credit opinion history tables (if applicable), are available for compendium reports and all J.P. Morgan–covered companies, and certain non-covered companies, by visiting research.disclosures.industries@jpmorgan.com

History of Investment Recommendations:
A history of J.P. Morgan investment recommendations disseminated during the preceding 12 months can be accessed on the Research & Commentary page of http://www.jpmorganmarkets.com where you can also search by analyst name, sector or financial instrument.

Analysts' Compensation: The research analysts responsible for the preparation of this report receive compensation based upon various factors, including the quality and accuracy of research, client feedback, competitive factors, and overall firm revenues.

Registration of non-US Analysts: Unless otherwise noted, the non-US analysts listed on the front of this report are employees of non-US affiliates of J.P. Morgan Securities LLC, may not be registered as research analysts under FINRA rules, may not be associated persons of J.P. Morgan Securities LLC, and may not be subject to FINRA Rule 2241 or 2242 restrictions on communications with covered companies, public appearances, and trading securities held by a research analyst account.

Other Disclosures

J.P. Morgan is a marketing name for investment banking businesses of JPMorgan Chase & Co. and its subsidiaries and affiliates worldwide.

UK MIFID FICC research unbundling exemption: UK clients should refer to UK MIFID Research Unbundling exemption for details of J.P. Morgan's implementation of the FICC research exemption and guidance on relevant FICC research categorisation.

All research material made available to clients are simultaneously available on our client website, J.P. Morgan Markets, unless specifically permitted by relevant laws. Not all research content is redistributed, e-mailed or made available to third-party aggregators. For all research material available on a particular stock, please contact your sales representative.

Any long form nomenclature for references to China; Hong Kong; Taiwan; and Macau within this research material are Mainland China; Hong Kong SAR (China); Taiwan (China); and Macau SAR (China).

J.P. Morgan Research may, from time to time, write on issuers or securities targeted by economic or financial sanctions imposed or administered by the governmental authorities of the U.S., EU, UK or other relevant jurisdictions (Sanctioned Securities). Nothing in this report is intended to be read or construed as encouraging, facilitating, promoting or otherwise approving investment or dealing in such Sanctioned Securities. Clients should be aware of their own legal and compliance obligations when making investment decisions.

Any digital or crypto assets discussed in this research report are subject to a rapidly changing regulatory landscape. For relevant regulatory advisories on crypto assets, including bitcoin and ether, please see https://www.jpmorgan.com/disclosures/cryptoasset-disclosure.

The author(s) of this research report may not be licensed to carry on regulated activities in your jurisdiction and, if not licensed, do not hold themselves out as being able to do so.

Exchange-Traded Funds (ETFs): J.P. Morgan Securities LLC ("JPMS") acts as authorized participant for substantially all U.S.-listed ETFs. To the extent that any ETFs are mentioned in this report, JPMS may earn commissions and transaction-based compensation in connection with the distribution of those ETF shares and may earn fees for performing other trade-related services, such as securities lending to short sellers of the ETF shares. JPMS may also perform services for the ETFs themselves, including acting as a broker or dealer to the ETFs. In addition, affiliates of JPMS may perform services for the ETFs, including trust, custodial, administration, lending, index calculation and/or maintenance and other services.

Options and Futures related research: If the information contained herein regards options- or futures-related research, such information is available only to persons who have received the proper options or futures risk disclosure documents. Please contact your J.P. Morgan Representative or visit https://www.theocc.com/components/docs/riskstoc.pdf for a copy of the Option Clearing Corporation's Characteristics and Risks of Standardized Options or https://www.finra.org/sites/default/files/2020-08/Security_Futures_Risk_Disclosure_Statement_2020.pdf for a copy of the Security Futures Risk Disclosure Statement.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/global/disclosures/interbank_offered_rates

Private Bank Clients: Where you are receiving research as a client of the private banking businesses offered by JPMorgan Chase & Co. and its subsidiaries ("J.P. Morgan Private Bank"), research is provided to you by J.P. Morgan Private Bank and not by any other division of J.P. Morgan, including, but not limited to, the J.P. Morgan Corporate and Investment Bank and its Global Research division.

Legal entity responsible for the production and distribution of research: The legal entity identified below the name of the Reg AC Research Analyst who authored this material is the legal entity responsible for the production of this research. Where multiple Reg AC Research Analysts authored this material with different legal entities identified below their names, these legal entities are jointly responsible for the production of this research. Where more than one legal entity is listed under an analyst's name, the first legal entity is responsible for the production unless stated otherwise. Research Analysts from various J.P. Morgan affiliates may have contributed to the production of this material but may not be licensed to carry out regulated activities in your jurisdiction (and do not hold themselves out as being able to do so). Unless otherwise stated below in the legal entity disclosures, this material has been distributed by the legal entity responsible for production, or where more than one

legal entity is listed under the analyst's name, the first legal entity will be responsible for distribution. If you have any queries, please contact the relevant Research Analyst in your jurisdiction or the entity in your jurisdiction that has distributed this research material.

Legal Entities Disclosures and Country-/Region-Specific Disclosures:
Argentina: JPMorgan Chase Bank N.A Sucursal Buenos Aires is regulated by Banco Central de la República Argentina ("BCRA"- Central Bank of Argentina) and Comisión Nacional de Valores ("CNV"- Argentinian Securities Commission - ALYC y AN Integral N°51).

Australia: J.P. Morgan Securities Australia Limited ("JPMSAL") (ABN 61 003 245 234/AFS Licence No: 238066) is regulated by the Australian Securities and Investments Commission and is a Market Participant of ASX Limited, a Clearing and Settlement Participant of ASX Clear Pty Limited and a Clearing Participant of ASX Clear (Futures) Pty Limited. This material is issued and distributed in Australia by or on behalf of JPMSAL only to "wholesale clients" (as defined in section 761G of the Corporations Act 2001). A list of all financial products covered can be found by visiting https://www.jpmm.com/research/disclosures. J.P. Morgan seeks to cover companies of relevance to the domestic and international investor base across all Global Industry Classification Standard (GICS) sectors, as well as across a range of market capitalisation sizes. If applicable, in the course of conducting public side due diligence on the subject company(ies), the Research Analyst team may at times perform such diligence through corporate engagements such as site visits, discussions with company representatives, management presentations, etc. Research issued by JPMSAL has been prepared in accordance with J.P. Morgan Australia's Research Independence Policy which can be found at the following link: J.P. Morgan Australia - Research Independence Policy.

Brazil: Banco J.P. Morgan S.A. is regulated by the Comissao de Valores Mobiliarios (CVM) and by the Central Bank of Brazil. Ombudsman J.P. Morgan: 0800-7700847 / 0800-7700810 (For Hearing Impaired) / ouvidoria.jp.morgan@jpmchase.com.

Canada: J.P. Morgan Securities Canada Inc. is a registered investment dealer, regulated by the Canadian Investment Regulatory Organization and the Ontario Securities Commission and is the participating member on Canadian exchanges. This material is distributed in Canada by or on behalf of J.P.Morgan Securities Canada Inc.

Chile: Inversiones J.P. Morgan Limitada is an unregulated entity incorporated in Chile.

China: J.P. Morgan Securities (China) Company Limited has been approved by CSRC to conduct the securities investment consultancy business.

Colombia: Banco J.P. Morgan Colombia S.A. is supervised by the Superintendencia Financiera de Colombia (SFC). Any reference in this material to products or services offered abroad by entities other than the Bank in Colombia is included exclusively for descriptive purposes. Such references do not constitute, and should not be construed as, promotional activity or the provision of financial products or services within Colombian territory, as defined under applicable Colombian regulation.

Dubai International Financial Centre (DIFC): JPMorgan Chase Bank, N.A., Dubai Branch is regulated by the Dubai Financial Services Authority (DFSA) and its registered address is Dubai International Financial Centre - The Gate, West Wing, Level 3 and 9 PO Box 506551, Dubai, UAE. This material has been distributed by JP Morgan Chase Bank, N.A., Dubai Branch to persons regarded as professional clients or market counterparties as defined under the DFSA rules.

European Economic Area (EEA): Unless specified to the contrary, research is distributed in the EEA by J.P. Morgan SE ("JPM SE"), which is authorised as a credit institution by the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) and jointly supervised by the BaFin, the German Central Bank (Deutsche Bundesbank) and the European Central Bank (ECB). JPM SE is a company headquartered in Frankfurt with registered address at TaunusTurm, Taunustor 1, Frankfurt am Main, 60310, Germany. The material has been distributed in the EEA to persons regarded as professional investors (or equivalent) pursuant to Art. 4 para. 1 no. 10 and Annex II of MiFID II and its respective implementation in their home jurisdictions ("EEA professional investors"). This material must not be acted on or relied on by persons who are not EEA professional investors. Any investment or investment activity to which this material relates is only available to EEA relevant persons and will be engaged in only with EEA relevant persons.

Hong Kong: J.P. Morgan Securities (Asia Pacific) Limited (CE number AAJ321) is regulated by the Hong Kong Monetary Authority and the Securities and Futures Commission in Hong Kong, and J.P. Morgan Broking (Hong Kong) Limited (CE number AAB027) is regulated by the Securities and Futures Commission in Hong Kong. JP Morgan Chase Bank, N.A., Hong Kong Branch (CE Number AAL996) is regulated by the Hong Kong Monetary Authority and the Securities and Futures Commission, is organized under the laws of the United States with limited liability. Where the distribution of this material is a regulated activity in Hong Kong, the material is distributed in Hong Kong by or through J.P. Morgan Securities (Asia Pacific) Limited and/or J.P. Morgan Broking (Hong Kong) Limited.

India: J.P. Morgan India Private Limited (Corporate Identity Number - U67120MH1992FTC068724), having its registered office at J.P. Morgan Tower, Off. C.S.T. Road, Kalina, Santacruz - East, Mumbai – 400098, is registered with the Securities and Exchange Board of India (SEBI) as a 'Research Analyst' having registration number INH000001873. J.P. Morgan India Private Limited is also registered with SEBI as a member of the National Stock Exchange of India Limited and the Bombay Stock Exchange Limited (SEBI Registration Number – INZ000239730) and as a Merchant Banker (SEBI Registration Number - MB/INM000002970). Telephone: 91-22-6157 3000, Facsimile: 91-22-6157 3990 and Website: http://www.jpmipl.com. JPMorgan Chase Bank, N.A. - Mumbai Branch is licensed by the Reserve Bank of India (RBI) (Licence No. 53/ Licence No. BY.4/94; SEBI - IN/CUS/014/ CDSL : IN-DP-CDSL-444-2008/ IN-DP-NSDL-285-2008/ INBI00000984/ INE231311239) as a Scheduled Commercial Bank in India, which is its primary license allowing it to carry on Banking business in India and other activities, which a Bank branch in India are permitted to undertake. For non-local research material, this material is not distributed in India by J.P. Morgan India Private Limited. Compliance Officer: Ashutosh Sharma; ashutosh.j.sharma@jpmchase.com; +912261575002. Grievance Officer: Ramprasadh

K, jpmipl.research.feedback@jpmorgan.com; +912261573000. Registration granted by SEBI and certification from NISM in no way guarantee performance of the intermediary or provide any assurance of returns to investors. Please visit Terms and Conditions and Most Important Terms and Conditions (MITC). The annual Compliance audit report is available at http://www.jpmipl.com/#research.

Indonesia: PT J.P. Morgan Sekuritas Indonesia is a member of the Indonesia Stock Exchange and is registered and supervised by the Otoritas Jasa Keuangan (OJK).

Korea: J.P. Morgan Securities (Far East) Limited, Seoul Branch, is a member of the Korea Exchange (KRX). JPMorgan Chase Bank, N.A., Seoul Branch, is licensed as a branch office of foreign bank (JPMorgan Chase Bank, N.A.) in Korea. Both entities are regulated by the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS). For non-macro research material, the material is distributed in Korea by or through J.P. Morgan Securities (Far East) Limited, Seoul Branch.

Japan: JPMorgan Securities Japan Co., Ltd. and JPMorgan Chase Bank, N.A., Tokyo Branch are regulated by the Financial Services Agency in Japan.

Malaysia: This material is issued and distributed in Malaysia by JPMorgan Securities (Malaysia) Sdn Bhd (18146-X), which is a Participating Organization of Bursa Malaysia Berhad and holds a Capital Markets Services License issued by the Securities Commission in Malaysia.

Mexico: J.P. Morgan Casa de Bolsa, S.A. de C.V., J.P. Morgan Grupo Financiero is member of the Mexican Stock Exchange ("Bolsa Mexicana de Valores") and the Institutional Stock Exchange ("Bolsa Institucional de Valores"), and it is authorized to act as a broker dealer by the National Banking and Securities Exchange Commission ("Comisión Nacional Bancaria y de Valores").

New Zealand: This material is issued and distributed by JPMSAL in New Zealand only to "wholesale clients" (as defined in the Financial Markets Conduct Act 2013). JPMSAL is registered as a Financial Service Provider under the Financial Service providers (Registration and Dispute Resolution) Act of 2008.

Philippines: J.P. Morgan Securities Philippines Inc. is a Trading Participant of the Philippine Stock Exchange and a member of the Securities Clearing Corporation of the Philippines and the Securities Investor Protection Fund. It is regulated by the Securities and Exchange Commission.

Singapore: This material is issued and distributed in Singapore by or through J.P. Morgan Securities Singapore Private Limited (JPMSS) [MDDI (P) 057/08/2025 and Co. Reg. No.: 199405335R], which is a member of the Singapore Exchange Securities Trading Limited, and/or JPMorgan Chase Bank, N.A., Singapore branch (JPMCB Singapore), both of which are regulated by the Monetary Authority of Singapore. This material is issued and distributed in Singapore only to accredited investors, expert investors and institutional investors, as defined in Section 4A of the Securities and Futures Act, Cap. 289 (SFA). This material is not intended to be issued or distributed to any retail investors or any other investors that do not fall into the classes of "accredited investors," "expert investors" or "institutional investors," as defined under Section 4A of the SFA. Recipients of this material in Singapore are to contact JPMSS or JPMCB Singapore in respect of any matters arising from, or in connection with, the material.

South Africa: J.P. Morgan Equities South Africa Proprietary Limited and JPMorgan Chase Bank, N.A., Johannesburg Branch are members of the Johannesburg Securities Exchange and are regulated by the Financial Services Conduct Authority (FSCA).

Taiwan: J.P. Morgan Securities (Taiwan) Limited is a participant of the Taiwan Stock Exchange (company-type) and regulated by the Taiwan Securities and Futures Bureau. Material relating to equity securities is issued and distributed in Taiwan by J.P. Morgan Securities (Taiwan) Limited, subject to the license scope and the applicable laws and the regulations in Taiwan. **To the extent that J.P. Morgan Securities (Taiwan) Limited produces research materials on securities not listed on the Taiwan Stock Exchange or Taipei Exchange ("Non-Taiwan Listed Securities"), these materials shall not constitute securities recommendations for the purpose of applicable Taiwan regulations, and, for the avoidance of doubt, J.P. Morgan Securities (Taiwan) Limited does not act as broker for Non-Taiwan Listed Securities.** According to Paragraph 2, Article 7-1 of Operational Regulations Governing Securities Firms Recommending Trades in Securities to Customers (as amended or supplemented) and/or other applicable laws or regulations, please note that the recipient of this material is not permitted to engage in any activities in connection with the material that may give rise to conflicts of interests, unless otherwise disclosed in the "Important Disclosures" in this material.

Thailand: This material is issued and distributed in Thailand by JPMorgan Securities (Thailand) Ltd., which is a member of the Stock Exchange of Thailand and is regulated by the Ministry of Finance and the Securities and Exchange Commission. The registered address is 548 One City Center Building, 50th Floor, Ploenchit Road, Lumphini, Pathum Wan, Bangkok 10330.

UK: Research is produced in the UK by J.P. Morgan Securities plc ("JPMS plc") which is a member of the London Stock Exchange and is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority or J.P. Morgan Markets Limited ("JPMML Ltd") which is authorised and regulated by the Financial Conduct Authority. Unless specified to the contrary, this material is distributed in the UK by JPMS plc and is directed in the UK only to: (a) persons having professional experience in matters relating to investments falling within article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) (Order) 2005 ("the FPO"); (b) persons outlined in article 49 of the FPO (high net worth companies, unincorporated associations or partnerships, the trustees of high value trusts, etc.); or (c) any persons to whom this communication may otherwise lawfully be made; all such persons being referred to as "UK relevant persons". This material must not be acted on or relied on by persons who are not UK relevant persons. Any investment or investment activity to which this material relates is only available to UK relevant persons and will be engaged in only with UK relevant persons. A description of J.P. Morgan EMEA's policy for prevention and avoidance of conflicts of interest related to the production of Research can be found at the following link: J.P. Morgan EMEA - Research Independence Policy.

U.S.: J.P. Morgan Securities LLC ("JPMS") is a member of the NYSE, FINRA, SIPC, and the NFA. JPMorgan Chase Bank, N.A. is a member of the FDIC. Material published by non-U.S. affiliates is distributed in the U.S. by JPMS who accepts responsibility for its content.

General: Additional information is available upon request. The information in this material has been obtained from sources believed to be reliable. While all reasonable care has been taken to ensure that the facts stated in this material are accurate and that the forecasts, opinions and expectations contained herein are fair and reasonable, JPMorgan Chase & Co. or its affiliates and/or subsidiaries (collectively J.P. Morgan) make no representations or warranties whatsoever to the completeness or accuracy of the material provided, except with respect to any disclosures relative to J.P. Morgan and the Research Analyst's involvement with the issuer that is the subject of the material. Accordingly, no reliance should be placed on the accuracy, fairness or completeness of the information contained in this material. There may be certain discrepancies with data and/or limited content in this material as a result of calculations, adjustments, translations to different languages, and/or local regulatory restrictions, as applicable. These discrepancies should not impact the overall investment analysis, views and/or recommendations of the subject company(ies) that may be discussed in the material. Artificial intelligence tools may have been used in the preparation of this material, including assisting in data analysis, pattern recognition, and content drafting for research material. J.P. Morgan accepts no liability whatsoever for any loss arising from any use of this material or its contents, and neither J.P. Morgan nor any of its respective directors, officers or employees, shall be in any way responsible for the contents hereof, apart from the liabilities and responsibilities that may be imposed on them by the relevant regulatory authority in the jurisdiction in question, or the regulatory regime thereunder. Opinions, forecasts or projections contained in this material represent J.P. Morgan's current opinions or judgment as of the date of the material only and are therefore subject to change without notice. Periodic updates may be provided on companies/industries based on company-specific developments or announcements, market conditions or any other publicly available information. There can be no assurance that future results or events will be consistent with any such opinions, forecasts or projections, which represent only one possible outcome. Furthermore, such opinions, forecasts or projections are subject to certain risks, uncertainties and assumptions that have not been verified, and future actual results or events could differ materially. The value of, or income from, any investments referred to in this material may fluctuate and/or be affected by changes in exchange rates. All pricing is indicative as of the close of market for the securities discussed, unless otherwise stated. Past performance is not indicative of future results. Accordingly, investors may receive back less than originally invested. This material is not intended as an offer or solicitation for the purchase or sale of any financial instrument. The opinions and recommendations herein do not take into account individual client circumstances, objectives, or needs and are not intended as recommendations of particular securities, financial instruments or strategies to particular clients. This material may include views on structured securities, options, futures and other derivatives. These are complex instruments, may involve a high degree of risk and may be appropriate investments only for sophisticated investors who are capable of understanding and assuming the risks involved. The recipients of this material must make their own independent decisions regarding any securities or financial instruments mentioned herein and should seek advice from such independent financial, legal, tax or other adviser as they deem necessary. J.P. Morgan may trade as a principal on the basis of the Research Analysts' views and research, and it may also engage in transactions for its own account or for its clients' accounts in a manner inconsistent with the views taken in this material, and J.P. Morgan is under no obligation to ensure that such other communication is brought to the attention of any recipient of this material. Others within J.P. Morgan, including Strategists, Sales staff and other Research Analysts, may take views that are inconsistent with those taken in this material. Employees of J.P. Morgan not involved in the preparation of this material may have investments in the securities (or derivatives of such securities) mentioned in this material and may trade them in ways different from those discussed in this material. This material is not an advertisement for or marketing of any issuer, its products or services, or its securities in any jurisdiction.

Confidentiality and Security Notice: This transmission may contain information that is privileged, confidential, legally privileged, and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of the information contained herein (including any reliance thereon) is STRICTLY PROHIBITED. Although this transmission and any attachments are believed to be free of any virus or other defect that might affect any computer system into which it is received and opened, it is the responsibility of the recipient to ensure that it is virus free and no responsibility is accepted by JPMorgan Chase & Co., its subsidiaries and affiliates, as applicable, for any loss or damage arising in any way from its use. If you received this transmission in error, please immediately contact the sender and destroy the material in its entirety, whether in electronic or hard copy format. This message is subject to electronic monitoring: https://www.jpmorgan.com/disclosures/email

MSCI: Certain information herein ("Information") is reproduced by permission of MSCI Inc., its affiliates and information providers ("MSCI") ©2026. No reproduction or dissemination of the Information is permitted without an appropriate license. MSCI MAKES NO EXPRESS OR IMPLIED WARRANTIES (INCLUDING MERCHANTABILITY OR FITNESS) AS TO THE INFORMATION AND DISCLAIMS ALL LIABILITY TO THE EXTENT PERMITTED BY LAW. No Information constitutes investment advice, except for any applicable Information from MSCI ESG Research. Subject also to msci.com/disclaimer

Sustainalytics: Certain information, data, analyses and opinions contained herein are reproduced by permission of Sustainalytics and: (1) includes the proprietary information of Sustainalytics; (2) may not be copied or redistributed except as specifically authorized; (3) do not constitute investment advice nor an endorsement of any product or project; (4) are provided solely for informational purposes; and (5) are not warranted to be complete, accurate or timely. Sustainalytics is not responsible for any trading decisions, damages or other losses related to it or its use. The use of the data is subject to conditions available at https://www.sustainalytics.com/legal-disclaimers. ©2026 Sustainalytics. All Rights Reserved.

"Other Disclosures" last revised May 16, 2026.

Copyright 2026 JPMorgan Chase & Co. All rights reserved. This material or any portion hereof may not be reprinted, sold or redistributed without the written consent of J.P. Morgan. It is strictly prohibited to use or share without prior written consent from J.P.

Morgan any research material received from J.P. Morgan or an authorized third-party ("J.P. Morgan Data") in any third-party artificial intelligence ("AI") systems or models when such J.P. Morgan Data is accessible by a third-party.

Completed 28 Jun 2026 06:47 PM BST

Disseminated 29 Jun 2026 12:15 AM BST