Testimony of Jeanette Manfra
VP, Head of Risk and Compliance, Google Cloud
U.S. House Committee on Financial Services
December 10, 2025

Chairman Hill, Ranking Member Waters, and distinguished Members of the Committee; thank you for the opportunity to appear before you today. My name is Jeanette Manfra, and I am the Vice President of Risk and Compliance at Google Cloud. We appreciate the House Committee on Financial Services holding this important hearing, and we look forward to sharing Google's perspective on the opportunity that artificial intelligence provides to America's financial sector.

Artificial Intelligence in the Financial Sector: Identifying Opportunities and Mitigating Risks

Google believes that the introduction of artificial intelligence (AI) in the financial services sector promises to usher in a transformative era for quality, accessibility, efficiency, and compliance in financial markets and services. AI offers many benefits, including the potential to enhance individual productivity, strengthen security operations, and drive data-based decision-making and operational efficiencies. AI can automate repetitive tasks such as responding to requests for proposals, localizing multilingual content, and conducting compliance checks. It can help handle complex, unstructured data, enabling firms to extract valuable insights through advanced conversational interfaces and data summarization techniques and facilitating informed decision-making and strategic planning. And it can prioritize critical threats, automate routine tasks, and improve threat detection and vulnerability management–enabling analysts to focus on significant issues, reducing burnout, and shifting security operations from reactive to proactive, ultimately improving overall security efficiency. Aggregate efficiency and productivity gains due to AI initiatives across the banking sector are forecast to be substantial, with estimates suggesting a potential addition of up to $340 billion annually to the banking sector alone. Multinational corporations across many industries, including financial institutions, are exploring or already taking advantage of AI-based models.

At the same time, AI introduces risks that must be managed and mitigated. Google believes that existing risk management frameworks and established governance practices can be applied to manage risks in the AI context. In light of the unique complexities and potential impacts of AI, however, these models and frameworks may require regulatory clarifications to help firms effectively manage the new types of risks introduced by these advanced AI systems. In a recent report on AI risks in the financial management context, Google identified three key areas in which regulatory clarity can benefit all stakeholders. First, risk management guidance should specify documentation expectations for AI models. Second, regulators should take into account developers' use of practices such as grounding and outcome-based model evaluations, in addition to model explainability and transparency, in establishing the safety and soundness of AI-based models. Finally, regulators should recognize a set of controls, including continuous monitoring, robust testing protocols, and human-in-the-loop oversight, that are appropriate for ensuring the responsible deployment of AI in financial services.

Google's Efforts to Utilize Artificial Intelligence to Combat Money Laundering, Fraud, and Scams

Google fights scams and fraud with consumer tools and enterprise offerings by taking proactive measures to protect users from harm, deliver reliable information, and partner to create a safer internet. For more than a decade, Google has used advancements in AI to further protect people from online scams where malicious actors deceive users to gain access to money, personal information, or both. For example:

- Our advancements in AI anomaly detection help companies identify, or even predict, abnormal patterns in unbounded data streams. Whether the companies are a large retailer identifying positive buying behaviors, a financial services provider detecting fraud, or a telecommunications company identifying and mitigating potential threats, they can use our tools to help detect behavioral patterns that provide useful insights.

- With Google Cloud's Anti-Money Laundering (AML) AI, we provide a consolidated machine learning (ML)-generated customer risk score as an alternative to traditional transaction alerting. The risk score is based on the bank's data including transactional patterns, network behavior, and Know Your Customer (KYC) data to identify instances and groups of high-risk retail and commercial customers. The product can adapt to changes in underlying data, delivering more accurate results, which increases overall program effectiveness and improves operational efficiency.

- In Search, AI helps us detect and block hundreds of millions of scam-results every day. We have made major investments in our AI-powered scam-detection systems that have enabled us to catch 20 times the number of scam-filled pages. These improvements help ensure that Search results are legitimate and protect users from harmful sites trying to steal sensitive data. We also provide tools like "About this result," which lets users learn more about online sources before clicking into them.

- Our Android ecosystem automatically filters out phishing messages and scam calls. All apps in Android Play are scanned daily for continued security. Proactive protections warn users before users visit an identified dangerous site, and theft protection keeps users' data safe before, during, and after theft attempts. Android's scam defenses protect users around the world from over 10 billion suspected malicious calls and messages every month. We are also launching new features on Android like using AI to flag common scam messages like fake toll fees or package deliveries. We are also protecting people from malicious links and scams in Google Messages. And for victims of account compromise, we are making it safer and easier to regain access by expanding account recovery options with Recovery Contacts.

- Google Ads works to ensure the integrity of the ads on our platforms, protecting users and enabling a safe ecosystem for advertisers and publishers. We have developed, and regularly update, a range of policies and methods tailored to the ads ecosystem. In 2024, for example, we suspended over 39.2 million advertiser accounts, the vast majority of which were suspended before they ever served an ad; and we removed 5.1 billion bad ads globally. Our AI-powered models contributed to the detection and enforcement of 97% of the pages we took action on last year.

- In 2024, our AI-powered detection systems blocked or removed more than 12 million fake business profiles and over 240 million reviews that violated our policies. The vast majority of the misleading reviews were removed from Google Maps before they were ever seen by our users.

In addition to building Google products that are secure-by-design, we focus on preventing financial scams through the development and enforcement of our policies. For example, Google Ads has in place the Limited Ads Serving policy, which has been key to dramatically reducing the volume of scam ads.

We also enforce a set of global policies for all cryptocurrency-related advertising by requiring all advertisers to obtain Google certification and adhering to the local laws of the countries for which the advertisers target. We further explicitly prohibit advertisements for initial coin offerings, DeFi trading protocols, or otherwise promoting the purchase, sale, or trade of cryptocurrencies or related products. These policies create a robust framework that underscores our commitment to user safety and the integrity of our advertising ecosystem.

To enforce these policies, we began embedding researchers and AI approaches in Google cyber security teams more than a decade ago. More recently, we have developed a specialized large language model that is fine-tuned for security and threat-intelligence. Some of these new tools are already up to 70% better at detecting whether a file is malicious and up to 300% more effective at identifying files that exploit vulnerabilities. And AI learns quickly, helping defenders adapt to instances of financial crime, for example.

Google further disincentivizes this malicious behavior by proactively filing litigation to dismantle massive fraud operations. In a recent example, in November 2025, we announced our filing to dismantle "Lighthouse," a massive Phishing-as-a-Service operation. Bad actors built "Lighthouse" as a phishing-as-a-service kit to generate and deploy massive "smishing" (SMS phishing) attacks. These attacks exploit established brands like E-Z Pass to steal people's financial information. Our legal action is designed to dismantle the core infrastructure of this operation.

Collaboration Toward Responsible Artificial Intelligence Adoption

Whether to combat specific challenges like scams and fraud or to enable greater efficiency and productivity across society, responsible adoption of AI across sectors requires a collaborative approach among industry participants, regulatory bodies, and technology providers. Google has taken several steps to advance this objective.

We recognize that Google must work with partners to counter the critical threats posed by scams and frauds, and we are leading cross-industry efforts in combating fraud and scams in response, we have introduced the Agent Payments Protocol (AP2), an open-source protocol collaboratively developed with over 60 partners, including financial and technology companies like American Express, Mastercard, and PayPal. AP2 aims to standardize and secure transactions made by AI agents on behalf of users, addressing key challenges such as authorization, authenticity, and accountability. The protocol utilizes cryptographically-signed digital contracts called "Mandates" to create tamper-proof, verifiable records of user instructions for a variety of payment methods, from credit cards to cryptocurrencies. We expect AP2 to help foster new e-commerce experiences, such as automated purchasing, personalized offers, and streamlined travel bookings in a secure way.

Google has also introduced the Secure AI Framework (SAIF), a conceptual framework for secure AI systems, including those in the financial sector. And we have recently published an extension of the SAIF Risk Map to address the core operational components of agentic systems and their related risks and controls. SAIF has six core elements:

- **Expand strong security foundations to the AI ecosystem.** Leverage secure-by-default infrastructure protections and expertise built over the last two decades to protect AI systems, applications and users. At the same time, develop organizational expertise to keep pace with advances in AI and start to scale and adapt infrastructure protections in the context of AI and evolving threat models. For example, injection techniques like SQL injection have existed for some time, and organizations can adapt mitigations, such as input sanitization and limiting, to help better defend against prompt injection style attacks.

- **Extend detection and response to bring AI into an organization's threat universe.** Detect and respond to AI-related cyber incidents in time by extending threat intelligence and other capabilities. For organizations, this includes monitoring inputs and outputs of AI systems to detect anomalies, and using threat intelligence to anticipate attacks. This effort typically requires collaboration with trust and safety, threat intelligence, and counter abuse teams.

- **Automate defenses to keep pace with existing and new threats** Harness the latest AI innovations to improve the scale and speed of response efforts to security incidents. Adversaries will likely use AI to scale their impact, so it is important to use AI and its current and emerging capabilities to stay nimble and cost effective in protecting against them.

- **Harmonize platform level controls to ensure consistent security across the organization.** Align control frameworks to support AI risk mitigation and scale protections across different platforms and tools to ensure that the best protections are available to all AI applications in a scalable and cost efficient manner. At Google, this includes extending secure-by-default protections to AI platforms like Vertex AI and Security AI Workbench, and building controls and protections into the software development lifecycle. Capabilities that address general use cases, like Perspective API, can help the entire organization benefit from state of the art protections.

- **Adapt controls to adjust mitigations and create faster feedback loops for AI deployment.** Constantly test implementations through continuous learning and evolve detection and protections to address the changing threat environment. This includes techniques like reinforcement learning based on incidents and user feedback, and involves steps such as updating training data sets, fine-tuning models to respond strategically to attacks, and allowing the software that is used to build models to embed further security in context (e.g. detecting anomalous behavior). Organizations can also conduct regular Red Team exercises to improve safety assurance for AI-powered products and capabilities.

- **Contextualize AI system risks in surrounding business processes.** Conduct end-to-end risk assessments related to how organizations will deploy AI. This includes an assessment of the end-to-end business risk, such as data lineage, validation and operational behavior monitoring for certain types of applications. In addition, organizations should construct automated checks to validate AI performance.

In addition, Google co-founded the Coalition for Secure AI (CoSAI), an open-source initiative to help all developers and deployers of AI create and maintain secure by design AI systems and help advance the framework. CoSAI helps foster a collaborative ecosystem to share open-source methodologies, standardized frameworks, and tools. Since its launch, CoSAI has made significant strides in strengthening AI security in collaboration with industry and academia in areas including Software Supply Chain Security for AI Systems; Preparing

Defenders for a Changing Security Landscape; AI Security Risk Governance; and Secure Design Patterns for Agentic Systems.

Further, across Google Cloud, we model and promote the adoption of responsible AI data practices that preserve our customers' privacy and support their compliance journey. Robust privacy commitments outline how we protect user data and prioritize privacy and the greater adoption of artificial intelligence rearms their importance. We adhere to a holistic approach to AI risk management and compliance, including focusing on employing an AI risk assessment methodology for identifying, assessing, and mitigating risks; developing and using an automated, scalable, and evidence-based approach for auditing generative AI workloads; and emphasizing human oversight and collaboration in our risk assessments and governance councils.

Additionally, we use explainability tools to help understand and interpret AI predictions and evaluate potential bias; privacy-preserving technologies such as masking and tokenization and adhering to privacy laws; continuous monitoring and auditing for security vulnerabilities that AI might miss; investing in training programs to bridge the AI knowledge gap; and encouraging "interdisciplinary collaboration" between data scientists, risk analysts, and domain experts is also key.

Establishing Regulatory Harmony for Artificial Intelligence in the Financial Sector

Advances in AI have led to increased adoption in the financial services sector. A prominent use for this technology is to assist in key compliance and risk functions, including the detection of fraud, money laundering, and other financial crimes, as well as trade manipulation. As the use of these models grows, so do questions about managing risks associated with the models. In particular, regulators, financial institutions, and technology service providers have been looking at whether existing risk management guidance (“MRM Guidance”)—which has traditionally been the regulatory regime applicable to managing risk in the financial services industry—continues to be relevant for AI models and, if so, how the guidance should be interpreted and applied to this new technology.

Advances in AI technology hold substantial promise for the future of banking and financial services. These very same technologies could also transform how financial regulators supervise activities and markets, and safeguard consumers. While we commend regulators for providing a sound framework in existing MRM Guidance for identifying and mitigating potential risks posed by AI models, more can be done to increase certainty, clarity, and effective and efficient risk mitigation strategies.

Regulators should support the development of global standards and their use across the financial services and regulatory landscape by explicitly recognizing such standards as presumptive evidence of compliance with the MRM Guidance and sound AI risk mitigation practices. In addition, regulators should foster industry collaboration and training based on such standards.

We recognize that we alone cannot solve these challenges. We recently announced our endorsement of key bipartisan bills in the U.S. Congress – crucial bills that we believe will help bring a decisive end to the financial harm and damage wrought by foreign cybercriminals. As the world focuses on the potential of AI — and governments and industry work on a regulatory approach to ensure AI is safe and secure — we believe that AI represents an inflection point for digital security.

* * *

Thank you for convening this important hearing. We look forward to continuing to further raise awareness about cybersecurity threats and defenses for the financial sector and beyond.