



NAME OF REGISTRANT: TEXAS INSTRUMENTS INCORPORATED
NAME OF PERSON RELYING ON EXEMPTION: FRIENDS FIDUCIARY CORPORATION
ADDRESS OF PERSON RELYING ON EXEMPTION: 1700 MARKET STREET, SUITE 1535, PHILADELPHIA, PA 19103

The proponents are not required by SEC rules to file this communication but are doing so voluntarily.

March 20, 2024

To Texas Instruments Incorporated (TI) Stockholders:

Friends Fiduciary Corporation, along with co-filers Mercy Investment Services, Portico Benefit Services, and Presbyterian Church USA, seeks your support for the Proposal titled “Stockholder proposal to report on due diligence efforts to identify risks associated with product misuse,” at the stockholder meeting on April 25, 2024.

RESOLVED: Shareholders request that the Board of Directors commission an independent third-party report, at reasonable expense and excluding proprietary information, on Texas Instruments’ (TI) due diligence process to determine whether customers’ misuse of its products expose the company to human rights and other material risks.

**Rationale to vote FOR the Proposal
and Rebuttal to Company’s Opposition Statement**

Commissioning an independent third-party report regarding TI’s due diligence is in investors’ long-term best interests. This memorandum summarizes the rationale for shareholder support of the Proposal and describes how currently available information regarding TI’s governance, policies, and procedures for Know Your Customer (KYC) compliance, heightened human rights due diligence (hHRDD) for conflict-affected and high-risk areas (CAHRA), and sanctions and export controls are not sufficient for shareholders to assess current and future risks resulting from documented TI product misuse by sanctioned entities and other bad actors engaged in violations of international humanitarian and human rights law, including but not limited to the Russian invasion of Ukraine.

SUMMARY OF RATIONALE

- I. TI’s components and operations incur proximity to CAHRA and place the Company at risk of contributing or being linked to end-users’ violations of international law, exposing the Company to potential human rights, regulatory, and reputational risks.

- II. Non-Governmental Organizations have been able to trace deliveries of TI dual-use components for prohibited use; the Company needs to assess its policies and procedures for KYC, hHRDD, and export and sanctions controls, to mitigate risks.
- III. Publicly available information and disclosures about TI's governance policies and procedures for KYC compliance, hHRDD, and export and sanctions controls are insufficient.
- IV. The Proposal's requests would not micromanage TI's business or inappropriately interfere with TI's business operations, rather the requested report would improve transparency for investors and better align our Company's policies and practices to fulfill TI's commitment as articulated in "Living Our Values."¹

I. TI's components and operations incur proximity to CAHRA and place the Company at risk of contributing or being linked to end-users' violations of international law, exposing the Company to potential human rights, regulatory, and reputational risks.

TI's commercial and dual-use components are at high-risk for application in military systems used in CAHRA, including those areas directly impacted by the Russia/Ukraine war. As noted in TI's *Opposition Statement*, the Company recognizes the existence of "bad actors who seek to evade applicable laws and misuse our products for illicit and unauthorized uses." Manufacturing and distributing products that have a documented history of use in weapons systems in CAHRA incurs significant risk of proximity to end-users' violations of international law such as the deliberate targeting of civilians and civilian infrastructure by the Russian military in Ukraine.²

According to the Royal United Services Institute (RUSI) and the Department for Strategic Communications at the Apparatus of the Commander-in-Chief of the Armed Forces of Ukraine, the Company's components have been linked to weapons systems used by the Russian military against Ukraine.³ TI's *Opposition Statement* states that the longevity of the Company's chips, which can last for decades, means that, "even today, chips shipped before the Russian invasion of Ukraine are likely sitting unused in storerooms around the globe" and TI representatives have stated that the products found in these reports are all commercially available. However, as stated in the RUSI report, a number of the TI chips found in Russian and Iranian weapons systems were manufactured more recently and are classified under EAR99 U.S. export controls, which imposes "a due-diligence obligation to make sure they were not destined for a prohibited end user, or to be used in prohibited end use."⁴ Further, while the Company states that it "stopped selling products into Russia in February of 2022," Reuters reportedly found nearly 1,300 additional shipments of TI parts to Russia by third-party sellers.⁵

¹ Texas Instruments, "Living Our Values: TI's ambitions, values, and code of conduct," <https://www.ti.com/lit/ml/szzb178/szzb178.pdf> (accessed March 15, 2024).

² Natasha Bertrand, "CNN Exclusive: A single Iranian attack drone found to contain parts from more than a dozen US companies," *CNN*, January 4, 2023, <https://www.cnn.com/2023/01/04/politics/iranian-drone-parts-13-us-companies-ukraine-russia/index.html> (accessed March 15, 2024).

³ James Byrne, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds, and Jane Baker, "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," Royal United Services Institute, August 8, 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf (accessed March 15, 2024); "American CPUs found in Iran-made Kamikaze drones," *Ukrayinska Pravda*, September 26, 2022, <https://www.yahoo.com/video/american-cpus-found-iran-made-122325552.html> (accessed March 15, 2024).

⁴ *Ibid.*

⁵ David Gauthier-Villars, Steve Stecklow, Maurice Tamman, Stephen Grey, and Andrew MacAskill, "Special Report-As Russian missiles struck Ukraine, Western tech still flowed," *Reuters*, August 8, 2022, <https://www.reuters.com/article/ukraine-crisis-russia-missiles-chips/special-report-as-russian-missiles-struck-ukraine-western-tech-still-flowed-idUSL8N2ZJ087> (accessed March 15, 2024).

Despite TI's efforts to limit its exposure to the Russian market, reporting continues to show the Company's products inside Iranian drones that "Russia has been deploying across Ukraine against civilians and critical infrastructure."⁶ In a report provided to the United Nations, analysis conducted by NAKO (Independent Anti-Corruption Commission) found multiple components marked with the TI logo in Russian Kalibr missiles.⁷ According to research conducted by the Kyiv School of Economics (KSE), between January and October of 2023, \$140 million worth of battle related goods and \$142 million of critical TI components were imported into Russia.⁸ This KSE study reported TI's products represented 13 percent of all foreign components recovered on the battlefield in Ukraine, second most of all foreign manufacturers behind only Analog Devices (14 percent).

Prohibited end-users or end-use include embargoed countries, certain military actors, and microprocessors in military-use, specifically including cruise missiles, unmanned drones, and control, communication, and navigation systems.⁹ RUSI identified TI components in cruise missiles that struck non-military targets in Ukraine, such as critical infrastructure and urban population centers, considered violations of international humanitarian law (IHL).¹⁰ Attacks on Ukrainian civilians and civilian infrastructure with Russian and Iranian weapons systems deployed by the Russian military, specifically Iranian-made drones, have been widespread and severe with the Ukrainian government currently investigating more than 120,000 crimes of aggression and war crimes.¹¹

⁶ Natasha Bertrand, "Exclusive: Biden task force investigating how US tech ends up in Iranian attack drones used against Ukraine", *CNN*, December 21, 2022, <https://www.cnn.com/2022/12/21/politics/iranian-drones-russia-biden-task-force-us-tech-ukraine/index.html> (accessed March 15, 2024).; Nicole Cobler, "Iranian attack drone included parts made by 2 Texas companies," *Axios Austin*, January 5, 2023, <https://www.axios.com/local/austin/2023/01/05/iranian-attack-drone-texas-companies> (accessed March 15, 2023).

⁷ Ian Talley, "Ukrainian Analysis Identifies Western Supply Chain Behind Iran's Drones," *The Wall Street Journal*, November 16, 2022, <https://www.wsj.com/articles/ukrainian-analysis-identifies-western-supply-chain-behind-irans-drones-11668575332> (accessed March 15, 2024).

⁸ Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, Anna Vlasyuk, And Vladyslav Vlasiuk, "Challenges of Export Controls Enforcement," *Kyiv School of Economics*, January 2024 <https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf> (accessed March 15, 2024).

⁹ "15 CFR Part 744 - Control Policy: End-User and End-Use Based," Cornell Law School, <https://www.law.cornell.edu/cfr/text/15/part-744> (accessed March 15, 2024).

¹⁰ Stephanie van den Berg, "Explainer: When are attacks on civilian infrastructure war crimes?" *Reuters*, December 16, 2022, <https://www.reuters.com/world/europe/when-are-attacks-civilian-infrastructure-war-crimes-2022-12-16/> (accessed March 15, 2024).

¹¹ Офіційний твіттер Офісу Генерального прокурора / Prosecutor General's Office of Ukraine, Official Twitter [@GP_Ukraine] (2024, March 16) #RussianWarCrimes statistics for the past week: March 8 – 15, 2024. 590 new crimes registered. At least 535 children killed, 1 257 injured (the data without full consideration of places of active hostilities). [X]. X. https://x.com/GP_Ukraine/status/1768971553385943473 (accessed March 15, 2024).

This proximity of TI products to likely war crimes and crimes against humanity poses regulatory and reputational risk to the Company that could negatively impact long-term shareholder value. The Company states in its 2023 10-K the risks of, “improper, incorrect, illicit or unauthorized storage, handling, modification or use of our products (including applications for which our products were not designed) ... by third parties could result in reputational harm.”¹²

The U.S. Government (USG) has launched and recently expanded a task force adding 25 new prosecutors to its counterintelligence and exports controls section, focused on “the enforcement of export controls—regulations designed to keep sensitive technologies out of the hand of foreign adversaries.”¹³ The USG also included specific mention of the regulatory risks for companies providing dual-use “microelectronics used in Russian and Iranian drones and unmanned aerial vehicles when destined for Russia, Belarus, or Iran” in its recent Russia Business Advisory.¹⁴ Finally, a U.S. Senate panel held a hearing last month, focused on the use of U.S. chips in Russian weapons, during which the panel chair urged that semiconductor companies “have the capacity to trace and track those components well enough to do something more.”¹⁵

The Company also continues to receive media scrutiny, including a PBS *NewsHour* segment reporting on Russian long-range missiles fired into Ukrainian cities that contained components made by U.S. companies. This report highlighted TI components “turning up in multiple weapons platforms used by Russia.”¹⁶ *Bloomberg* also identified Texas Instruments as one of two of the biggest makers of chips that have “continued to flow to Russian military-linked companies this year in spite of export restrictions.”¹⁷ These reputational and regulatory risks could be mitigated by our Company through more rigorous human rights and know your customer due diligence processes.

¹² “Form 10-K,” Texas Instruments, United States Securities and Exchange Commission, December 31, 2023, <https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/0000097476/000009747624000007/txn-20231231.htm> (accessed March 15, 2024).

¹³ Dylan Tokar and Ian Talley, “Justice Department Hiring Dozens of New Prosecutors to Enforce Russian Sanctions,” *The Wall Street Journal*, March 2, 2023, <https://www.wsj.com/articles/justice-department-hiring-dozens-of-new-prosecutors-to-enforce-russian-sanctions-4e9b9047> (accessed March 15, 2024).

¹⁴ “Risks and Considerations for Doing Business in the Russian Federation and Russia-Occupied Territories of Ukraine,” *United States Department of State*, February 23, 2024, <https://www.state.gov/russia-business-advisory/> (accessed March 15, 2024).

¹⁵ Karen Freifeld, “US Senator urges chipmakers to help keep their chips out of Russian weapons,” *Reuters*, February 27, 2024, <https://www.reuters.com/technology/us-chipmakers-should-do-more-keep-chips-out-russian-weapons-senator-says-2024-02-27/> (accessed March 15, 2024).

¹⁶ Simon Ostrovsky, “Parts made by U.S. companies used to build Russian cruise missiles,” *PBS NewsHour*, July 21, 2023, <https://www.pbs.org/newshour/show/parts-made-by-u-s-companies-used-to-build-russian-cruise-missiles> (accessed March 15, 2024).

¹⁷ Sheridan Prasso, “Chips From Texas Instruments and Other US Makers Flow Into Russia Despite Ban,” *Bloomberg*, December 21, 2023, <https://finance.yahoo.com/news/chips-texas-instruments-other-us-120000205.html> (accessed March 15, 2024).

II. Non-Governmental Organizations have been able to trace deliveries of TI dual-use components for prohibited use; the Company needs to assess its policies and procedures for KYC, hHRDD, and export and sanctions controls, to mitigate risks.

Filers acknowledge the complex reality of the semiconductor industry and the difficulties with transparency in its value chain. Filers also recognize the dual-use nature of semiconductor components, the industry's reliance on retail markets and third-party distributors, and the long lifespan of chips makes tracking the end-users of 80,000 distinct products practically unfeasible. However, TI's framing that our Company already gives a significant amount of time and resources to combat illicit diversion through their global trade compliance program and, as a result, has no further responsibility for more robust due diligence to safeguard against prohibited end-use of its dual-use products is at odds with our Company's commitment to "responsible business practices" as articulated in TI's "Living our Values." The Company's position is all the more concerning in the face of documented TI product proximity to on-going severe human rights abuses.

The Filers' proposal does not seek complete visibility into TI's value chain. Rather, the Filers' proposal asks for additional information regarding TI's policies and procedures to determine if the Company is adequately engaging in KYC compliance, conducting hHRDD for operations in CAHRA, and has the necessary governance and oversight to abide by its obligations under the United Nations Guiding Principles on Business and Human Rights (UNGPs). According to RUSI's report, Sertal LLC, a Russian based organization that has been found by the US Department of Justice to be "under the direction of Russian intelligence services to procure advanced electronics and sophisticated testing equipment for the Russian military industrial complex" publicly declared it was a supplier of electronic components manufactured by Texas Instruments. The report continues to describe that as recently as March 2021, Sertal LLC imported over \$600,000 worth of electronic integrated circuits from Texas Instruments.

The RUSI investigation highlights the fact that if non-governmental organizations can map TI's components from point of manufacture to point of end-use – in violation of international law in Ukraine – our Company should be able to conduct more effective due diligence and better limit bad actors' access to their products.

III. Publicly available information and disclosures about TI's governance policies and procedures for KYC compliance, hHRDD, and export and sanctions controls are insufficient.

The Company has developed a set of policies, disclosures, and reports regarding its business ethics, management of suppliers' human rights risks, environmental risks, expectations for employees, and public policy efforts.¹⁸ While Filers recognize these efforts to comply with corporate obligations under the UNGPs, TI's publicly available information fails to communicate how the Company mitigates its heightened risk of causing, contributing to, or being linked to conflict-related impacts and violations of international law that are associated with its customers' and end-users' application of its products.

TI's *Opposition Statement* states the Company has "a robust global trade compliance program which includes customer due diligence" that is "overseen by the audit committee of the board of directors." However, the Company's audit committee and Board lack membership with adequate human rights or conflict risk experience.¹⁹ TI has also scored low on the Corporate Human Rights Benchmark, with the Company's governance and policy commitments receiving a score of 0.5 out of 10.²⁰ This proposal seeks a third-party expert to analyze these policies, procedures, and outcomes as opposed to passively relying on TI's Board.

TI's *Opposition Statement* also states that "the requested report probes deeply into day-to-day business and compliance matters, which TI is managing appropriately and over which the board's audit committee is exercising effective oversight." However, given the recent investigations that found dozens of TI's unique components in Iranian and Russian weapons systems, the Company's existing compliance program and the related oversight function appear lacking. Ensuring Company procedures include KYC compliance and hHRDD for CAHRA and that the Company's export and sanctions controls are sufficiently robust is essential to mitigating risks and protecting investors' interests.²¹

¹⁸ Texas Instruments, "Corporate Citizenship," <https://www.ti.com/about-ti/citizenship-community/overview.html> (accessed March 15, 2024).

¹⁹ Texas Instruments, "Board of directors & committees," <https://investor.ti.com/corporate-governance/board-of-directors-committees> (accessed March 15, 2024).

²⁰ World Benchmarking Alliance, Corporate Human Rights Benchmark, "Texas Instruments," <https://www.worldbenchmarkingalliance.org/publication/chrbc/companies/texas-instruments-3/> (accessed March 15, 2024).

²¹ James Byrne, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds, and Jane Baker, "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," Royal United Services Institute, August 8, 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf (accessed March 15, 2024); "American CPUs found in Iran-made Kamikaze drones," *Ukrainska Pravda*, September 26, 2022, <https://www.yahoo.com/video/american-cpus-found-iran-made-122325552.html> (accessed March 15, 2024).

IV. The Proposal’s requests would not micromanage TI’s business or inappropriately interfere with TI’s business operations, rather the requested report would improve transparency for investors and better align our Company’s policies and practices to fulfill TI’s commitment as articulated in “Living Our Values.”

Filers’ proposal does not micromanage TI’s business or interfere with business operations, rather it encourages the Company to conduct a heightened level of human rights and KYC due diligence corresponding to the heightened potential regulatory, reputational, and financial risks to our Company through product misuse in Russia and other CAHRA. The proposal seeks non-proprietary information at a reasonable expense. In fact, the proposal specifically seeks a third-party to conduct the review and draft the report to obtain an expert opinion.

Information regarding a company’s human rights- and conflict-related risks is increasingly becoming material to investors as more evidence regarding corresponding financial impact becomes available. For example, investors representing over \$11 trillion in assets under management signed public statements concerning these risks in Ukraine,²² Myanmar,²³ and Xinjiang Autonomous Region, China.²⁴ Furthermore, “conflict risk” was the second leading environmental, social, and governance (ESG) criteria among institutional investors, according to The Forum for Sustainable and Responsible Investment’s 2022 *Report on US Sustainable, Responsible and Impact Investing Trends*.²⁵ The request to provide information and coordinate with a third-party expert is not overburdensome especially given the material nature of the information requested.

As long-term investors, the Filers believe that commissioning an independent third-party report regarding the Company’s due diligence is in investor’s long-term best interests and is not only compatible with but required by TI’s stated values in “Living Our Values,” specifically the commitment to responsible business practices, a long-term “ownership” perspective, and products and operations of which our Company can be proud.

We urge you to vote FOR the Proposal requesting an independent third-party report regarding TI’s due diligence process to determine whether its customers’ use of its products or services contribute or are linked to violations of international law.

Sincerely,

Jeffery Perkins
Executive Director
Friends Fiduciary Corporation

²² “Investor Statement on the Crisis in Ukraine,” Business & Human Rights Resource Centre, May 16, 2022, https://media.business-humanrights.org/media/documents/Investor_Statement_on_the_Crisis_in_Ukraine_16_May_2022.pdf (accessed February 22, 2023).

²³ “Investor Statement on Human Rights and Business Activities in Myanmar,” Business & Human Rights Resource Centre, June 9, 2021, <https://www.business-humanrights.org/en/latest-news/investor-statement-on-human-rights-and-business-activities-in-myanmar/> (accessed February 22, 2023).

²⁴ “Investor Expectations on Human Rights Crisis in the Xinjiang Uyghur Autonomous Region,” Investor Alliance for Human Rights, April 2022, <https://investorsforhumanrights.org/sites/default/files/attachments/2022-04/XUAR%20Investor%20Expectations%20Statement%20-%20April%202022.pdf> (accessed February 22, 2023).

²⁵ US SIF Foundation, “Report on US Sustainable, Responsible and Impact Investing Trends,” 2022 <https://www.ussif.org//Files/Trends/2022/Institutional%20Investors%202022.pdf>, (accessed on February 22, 2023).



This is not a solicitation of authority to vote your proxy. Please DO NOT send us your proxy card; neither Friends Fiduciary Corporation nor any of the co-filers are able to vote your proxies, nor does this communication contemplate such an event. Friends Fiduciary Corporation urges stockholders to vote for the Proposal following the instructions provided on the Company's proxy mailing.