

PROXY MEMORANDUM

To: Microchip Technology Incorporated Shareholders
Subject: 2024 Proxy Statement – Proposal Five: Independent Third-Party Report on Due Diligence Process to Determine Whether Customers’ Use of Products Contribute or are Linked to Violations of International Law
Date: July 16, 2024
Contact: Katie Carter, Director of Faith-Based Investing and Shareholder Engagement, Katie.Carter@pcusa.org

The Presbyterian Church (U.S.A.) filed Proxy Item No. 5. The proposal will be voted on at the August 20, 2024, Annual Meeting of Microchip Technology Incorporated (Microchip).

Resolved:

Shareholders request that the Board of Directors commission an independent third-party report, at reasonable expense and excluding proprietary information, on Microchip Technology Corporation’s (Microchip) due diligence process to determine whether its customers’ use of its products contribute or are linked to violations of international humanitarian law (IHL).

Commissioning an independent third-party report regarding Microchip’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 Microchip’s due diligence processes – Know Your Customer (KYC), human rights, and regulatory compliance – is insufficient for shareholders to assess current and future risks resulting from product misuse by sanctioned entities and other bad actors violating international law, including during the Russian invasion of Ukraine.

Summary of Rationale

1. Microchip’s components and operations expose the company to an increasing number of global conflicts, placing the Company at risk of contributing or being linked to end-users’ violations of international law and exposing it to potential human rights, regulatory, and reputational risks.
2. Publicly available information and disclosures about Microchip’s KYC, human rights, and regulatory compliance due diligence processes are insufficient and not aligned with evolving regulations or industry peers.
3. Non-governmental organizations (NGOs) have been able to more accurately trace deliveries of Microchip dual-use components for prohibited use than the company’s disclosures indicate; the Company must assess its due diligence processes to prevent and mitigate risks.
4. The Proposal’s request for an external report would not micromanage Microchip’s internal business operations but would assess and communicate to fellow shareholders to what extent Microchip’s due diligence processes are aligned with evolving industry practice, rapidly evolving regulations, and the company’s own Human Rights Policy¹ and Guiding Values².

1. Microchip’s components and operations incur proximity to an increasing number of global conflicts, placing the Company at risk of contributing or being linked to end-users’ violations of international law and exposing it to potential human rights, regulatory, and reputational risks.

Microchip’s commercial and dual-use components are at high risk for application in military systems used in conflict-affected areas (e.g., Ukraine), especially as product diversion continues to challenge the semiconductor industry and the demand for military-grade microelectronics increases alongside growing geopolitical conflict.³ This increase in conflict,⁴ the growing use of militarized drones and other dual-use systems, and the indispensability of microelectronics to these systems, has prompted heightened scrutiny and action from an array of stakeholders, including the U.S. Government (USG), members of Congress, investors, and media.

The USG continues to expand sanctions related to semiconductor diversion and misuse, both on Russian individuals and entities and secondary sanctions on resellers in China responsible for diversion to Russia.⁵ 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.⁶ Further, the U.S. Senate Permanent Subcommittee on Investigations held a hearing earlier this year, 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.”⁷

Meanwhile, the European Union (EU) passed mandatory human rights due diligence (HRDD) legislation, including the Corporate Sustainability Reporting Directive (CSRD)⁸ and Corporate Sustainability Due Diligence Directive (CSDDD),⁹ and EU Member States are passing similar legislation including France’s Duty of Vigilance Law, Germany’s Supply Chain Law, and Norway’s Transparency Act. These pieces of legislation require companies domiciled or operating in the EU, like Microchip, to conduct and disclose details concerning their HRDD processes beyond the Company’s current practices.

¹ “Human Rights Policy,” Microchip Technology, <https://ww1.microchip.com/downloads/aemDocuments/documents/financial/investordocuments/corporate-governance/HR-650-Human-Rights-Policy-2022.12.09.pdf> (accessed July 2, 2024).

² “Mission, Vision, and Guiding Values,” Microchip Technology, <https://ww1.microchip.com/downloads/aemDocuments/documents/financial/investordocuments/mission-statement/Mission-Vision-and-Guiding-Values.pdf> (accessed July 2, 2024).

³ Kathryn Ackerman, “Large Investments by Aerospace and Defense Industries in Microelectronics Are the New Normal,” Sourceability, February 14, 2024, <https://sourceability.com/post/large-investments-by-aerospace-and-defense-industries-in-microelectronics-are-the-new-normal> (accessed July 2, 2024).

⁴ ACLED Conflict Index, <https://acleddata.com/conflict-index/> (accessed July 2, 2024).

⁵ Josh Wingrove and Daniel Flatley, “US Expands Russia Sanctions to Target LNG Projects, Chips,” *Bloomberg*, June 11, 2024, <https://www.bloomberg.com/news/articles/2024-06-11/chip-sales-to-russia-to-be-curbed-under-wider-us-sanctions> (accessed July 2, 2024).

⁶ “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 July 2, 2024).

⁷ 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 July 2, 2024).

⁸ “Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022,” *Official Journal of the European Union*, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2464> (accessed July 2, 2024).

⁹ Corporate sustainability due diligence: Council gives its final approval,” Council of the EU, May 24, 2024, <https://www.consilium.europa.eu/en/press/press-releases/2024/05/24/corporate-sustainability-due-diligence-council-gives-its-final-approval/> (accessed July 2, 2024).

Institutional investors in North America and Europe continue to prioritize the issue of semiconductor diversion and misuse during conflict while engaging Microchip and a number of its industry peers.¹⁰ Relatedly, media reports continue to highlight the risks associated with Microchip and other companies' semiconductors being used during the Russian invasion two years into the war. This has included coverage of the role China plays as a diversion hub,¹¹ investigations into how diversion is financing Russian criminal networks,¹² and reporting on the ongoing indispensability of western semiconductors to the Russian war effort,¹³ most recently in a missile strike on a Ukrainian children's hospital.¹⁴

The Company acknowledges several of the challenges associated with preventing the use of its commercially available microelectronics by bad actors, noting in its Opposition Statement:

The challenge of preventing integrated circuit (IC) diversion is significant. ICs are ubiquitous, durable, small, and can be repurposed, making them susceptible to diversion. Bad actors may evade sanctions in order to obtain ICs.¹⁵

In addition, the Opposition Statement addresses the specific concerns of diversion related to the Russian invasion of Ukraine:

One analysis of Iranian drones recovered in Ukraine found that approximately half of the ICs had manufacturing dates in 2020 and 2021 (before Russia's invasion of Ukraine), and certain ICs dated back to 2005.(3) This means that ICs found in a conflict-affected area may have been purchased long before sanctions or export controls were imposed, and may have changed hands several times.¹⁶

¹⁰ Gina Gambetta, "Big Read: Are investors still holding corporations to account over Russia ties?" *Responsible Investor*, February 26, 2024, <https://www.responsible-investor.com/big-read-are-investors-still-holding-corporates-to-account-over-russia-ties/> (accessed July 2, 2024).

¹¹ "US Intelligence Finding Shows China Surging Equipment Sales to Russia to Help War Effort in Ukraine," *US News & World Report*, April 12, 2024, <https://www.usnews.com/news/world/articles/2024-04-12/us-intelligence-finding-shows-china-surging-equipment-sales-to-russia-to-help-war-effort-in-ukraine> (accessed July 2, 2024).

¹² Vanda Felbab-Brown and Diana Paz García, "Russia, Ukraine, and organized crime and illicit economies in 2024," Brookings, February 6, 2024, <https://www.brookings.edu/articles/russia-ukraine-and-organized-crime-and-illicit-economies-in-2024/> (accessed July 2, 2024).

¹³ Alberto Nardelli, "Most of Russia's War Chips Are Made by US and European Companies," *Bloomberg*, January 25, 2024, <https://www.bloomberg.com/news/articles/2024-01-25/russia-s-war-machine-powered-by-chips-from-intel-amd-infineon-stm> (accessed July 2, 2024).

¹⁴ Christopher Miller, Max Seddon, Chris Cook, Sam Joiner, Toru Tsunashima, and Chris Campbell, "Type of Russian missile that struck Kyiv children's hospital uses western components," *Financial Times*, July 10, 2024, <https://www.ft.com/content/ef463ac9-4804-4ad7-b9a2-c113590f2f96> (accessed July 12, 2024).

¹⁵ "2024 Proxy Statement - Company Opposition Statement to Proposal 5," Microchip Technology, June 25, 2024.

¹⁶ "2024 Proxy Statement - Company Opposition Statement to Proposal 5," Microchip Technology, June 25, 2024.

The Filers have also acknowledged, including during meetings with Microchip staff, how the volume of commercial semiconductors on the market, “legacy chips,” and counterfeiting are significant challenges to diversion prevention.

However, Microchip’s reliance on these challenges related to misuse in conflict-affected areas underscores the limitations of a due diligence process that is primarily focused or solely reliant on sanctions compliance. Best practices indicate that a compliance-based due diligence process is the legal minimum. While Russia did not launch a full-scale invasion of Ukraine until February 2022, the Putin regime had been unlawfully occupying Crimea and the Donbass region in contravention of international law since 2014, creating a heightened level of risk that necessitated a heightened level of due diligence. In other words, the risks associated with diversion and misuse by Russia did not begin with the full-scale invasion of Ukraine nor with the imposition of sanctions.

Despite Microchip’s efforts to limit its exposure to the Russian market since March 2022, according to research conducted by the Kyiv School of Economics (KSE) and the Yermak-McFaul International Working Group on Russian Sanctions, Microchip was among the top 15 companies whose “battlefield goods” – priority components identified by the USG, EU, and United Kingdom – were imported into Russia between January and October of 2023.¹⁷

Further, the Opposition Statement does not account for the diversion and misuse of Microchip’s dual-use products, including those for military purposes (e.g., “precision strike/missile defense, communications, radar, autonomous systems, joint all-domain command control, image processing”¹⁸). A number of these products 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.”¹⁹

¹⁷ Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Natalia Shapoval, Anna Vlasjuk, and Vladyslav Vlasjuk, “Challenges of Export Controls Enforcement: How Russia Continues to Import Components for its Military Production,” Kyiv School of Economics and Yermak-McFaul International Working Group on Russia Sanctions, January 2024, <https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf> (accessed July 2, 2024).

¹⁸ “Defense Applications,” Microchip Technology, <https://www.microchip.com/en-us/solutions/aerospace-and-defense/defense> (accessed July 2, 2024).

¹⁹ 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-finalupdated-web_1.pdf (accessed July 2, 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 July 2, 2024).

According to a report from the Royal United Services Institute (RUSI), Microchip's products were among the most prevalent in the 208 dual-use components recovered from 26 Russian weapons systems, including the Iskander 9M727 and the KH-101 ballistic and cruise missile systems.²⁰ Investigations also found Microchip's products in other weapons systems recovered from the Ukrainian battlefield, including Russian and Iranian drones,²¹ Russian T-72 tanks,²² and the Orlan-10 drone.²³ These drones have been used by the Russian military to target Ukrainian civilians and civilian infrastructure in violation of IHL.²⁴ Furthermore, the human costs of the use of Russian and Iranian weapons systems have been widespread and severe with the Ukrainian government currently investigating over 127,000 crimes of aggression and war crimes.²⁵

The proximity of Microchip products to likely war crimes and crimes against humanity poses an increasing number and severity of human rights, regulatory, and reputational risks to the Company that could negatively impact long-term shareholder value. The increase in geopolitical conflict, the regulatory responses of the USG and EU (e.g., sanctions, trade controls, Congressional oversight, mandatory due diligence legislation), and continued scrutiny of the semiconductor industry by media platforms all pose potentially material impacts for Microchip.

2. Publicly available information and disclosures about Microchip's KYC, human rights, and regulatory compliance due diligence processes are insufficient and not aligned with evolving regulations or industry peers.

Investor concerns regarding product diversion and misuse by Russia, Iran, and other bad actors involved in armed conflict can only be addressed through disclosures that provide an adequate level of detail concerning due diligence processes related to KYC, human rights, and regulatory compliance. While the Filers acknowledge that on July 7, 2023, Microchip released its "Position on Sales to Russia," the document restated the Company's decision to halt sales, expressed its concern regarding diversion and misuse, and noted that it works with the USG to address these risks. The position did not provide any details regarding KYC, human rights, or regulatory compliance – beyond stating that it complies with applicable sanctions and laws.²⁶

²⁰ James Byrne, Gary Somerville, Joseph 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 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf (accessed July 2, 2024).

²¹ Chris Livesay, "Russia is bombarding Ukraine with drones guided by U.S.-made technology, and the chips are still flowing," *CBS News*, January 4, 2023, <https://www.cbsnews.com/news/ukraine-war-russia-iranian-drones-us-made-technology-chips/> (accessed July 2, 2024).

²² Anton Mykytiuk, "How foreign microchips end up in Russian tanks despite sanctions," *Euromaidan Press*, September 28, 2022, <https://euromaidanpress.com/2022/09/28/how-foreign-microchips-end-up-in-russian-tanks-despite-sanctions/> (accessed July 2, 2024).

²³ Maria Zholobova, Stephen Gray, and Maurice Tamman, "The West has banned the sale of components for the production of weapons to Russia. But she successfully buys them," *The Independent*, December 15, 2022, <https://storage.googleapis.com/istories/stories/2022/12/15/zapad-zapretit-prodavati-rossii-komplektuyushchie-dlya-proizvodstva-oruzhiya-no-ona-ikh-uspeshno-pokupaet/index.html> (accessed July 2, 2024).

²⁴ Alisha Rahaman Sarkar, "US claims Iran-made 'kamikaze' drones used by Russia to bomb Ukraine breach international law," *The Independent*, October 18, 2022, <https://www.independent.co.uk/news/world/americas/us-kamikaze-drone-ukraine-russia-b2204841.html> (accessed July 2, 2024).

²⁵ Офіційний твіттер Офісу Генерального прокурора / Prosecutor General's Office of Ukraine, Official Twitter [@GP_Ukraine] (2024, March 15) #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 July 2, 2024).

²⁶ "Position on Russia and Trade Controls," Microchip Technology, July 7, 2023 <https://ww1.microchip.com/downloads/aemDocuments/documents/announcements/microchip-position-on-russia-and-trade-controls.pdf> (accessed July 2, 2024).

Microchip's ongoing lack of transparency concerning its due diligence processes and the absence of any mention of HRDD in the company policy or Opposition Statement are not aligned with industry peers, evolving regulation, or USG guidance. The listing of "customer due diligence," "securing necessary licenses," and "working with regulatory agencies" in the Opposition Statement is not a substitute for outlining non-privileged information concerning these and other standard and emerging practices.

Specifically, as has been communicated to Company staff during engagements with the Filers, industry peers are taking additional steps to prevent and mitigate human rights and other risks associated with product diversion and misuse. For example, American semiconductor company Qualcomm has implemented a Human Rights Working Group that is "composed of representatives from legal; procurement; corporate responsibility; government affairs; environmental, health and safety; diversity and inclusion; supply chain; ethics and compliance; and privacy and security." The working group reports regularly to senior management and the Board of Directors, indicating that human rights is considered a governance priority. Further, Qualcomm notes that it regularly conducts, "human rights impact assessments, including company-wide and within certain regions," and materiality assessments that identified "product misuse" as a salient human rights risk.²⁷

Similarly, Intel has multiple teams, including a cross functional human rights steering committee that are responsible for conducting due diligence and implementing policies and procedures to address salient human rights risks and support adherence to its human rights policy. Under "Product Responsibility," Intel notes:

Where we become aware of a concern that Intel products are being used by a business partner in connection with abuses of human rights, we will restrict or cease business with the third party until and unless we have high confidence that Intel's products are not being used to violate human rights.²⁸

Other peers have responded to shareholder concerns during engagements with commitments to conduct human rights impact assessments for their global operations and integrate human rights into KYC red flag indicators.

Microchip's current disclosures are also inadequate for the purpose of complying with recent mandatory due diligence legislation passed in the EU (e.g., CSRD, CSDDD) and across its Member States (France's Duty of Vigilance Law, Germany's Supply Chain Act, Norway's Transparency Act). For example, as reported by the Council of the European Union, CSDD will require:

... companies to ensure that human rights and environmental obligations are respected along their chain of activities. If a violation of these obligations is identified, companies will have to take the appropriate measures to prevent, mitigate, bring to an end or minimise the adverse impacts arising from their own operations, those of their subsidiaries and those of their business partners in their chain of activities. Companies can be held liable for the damage caused and will have to provide full compensation.²⁹

²⁷ "Human Rights Statement," Qualcomm, <https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/qualcomm-human-rights-statement.pdf> (accessed July 2, 2024).

²⁸ "Global Human Rights Policy," Intel, <https://www.intel.com/content/www/us/en/policy/policy-human-rights.html> (accessed July 2, 2024).

²⁹ "Corporate sustainability due diligence: Council gives its final approval," Council of the EU, May 24, 2024, <https://www.consilium.europa.eu/en/press/press-releases/2024/05/24/corporate-sustainability-due-diligence-council-gives-its-final-approval/> (accessed July 2, 2024).

Finally, the USG's Russia Business Advisory notes that due to the "significant operational, legal, economic, and reputational risks" associated with ongoing exposure to the Russian market, companies should conduct heightened due diligence to "reduce or mitigate these risks and facilitate increased transparency to all stakeholders regarding such risks."³⁰ Microchip's current disclosures do not adequately communicate how or if such heightened due diligence processes are being performed or communicated.

Without sufficient disclosure to address Filers' and other shareholders' concerns related to product diversion and misuse by Russia, Iran, and other bad actors and the potential human rights, regulatory, and reputational risks this conduct creates, it is imperative that a third party with relevant expertise be hired to assess Microchip's current due diligence processes.

3. Non-governmental organizations have more accurately traced deliveries of Microchip dual-use components for prohibited use than the company's disclosures indicate; the Company needs to assess its due diligence processes to prevent and mitigate risks.

The filers acknowledge the complex reality of the semiconductor industry including the difficulties associated with transparency in value chains. The 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 complete tracking of the end-users of tens of thousands of distinct products unfeasible. However, Microchip's framing that it already dedicates 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 Microchip's commitment to "Professional Ethics and Social Responsibility" as articulated in Microchip's "Guiding Values." The Company's position is even more concerning in the face of documented Microchip product proximity to on-going severe human rights abuses in Ukraine.

The Filers' proposal does not seek complete visibility into Microchip's value chain. Rather, it asks for additional information regarding Microchip's due diligence processes related to KYC, human rights, and regulatory compliance to ensure our Company is adequately addressing its regulatory and reputational risks and meeting its obligations under the United Nations Guiding Principles on Business and Human Rights. Investigative reporting as recent as April 2024 by the American Enterprise Institute and January 2024 by KSE and Yermak-McFaul indicate that significant amounts of commercial and dual-use Microchip products are being imported into Russia and used during the invasion of Ukraine.

Investigations by these organizations, media platforms, and RUSI highlight the fact that if NGOs can map Microchip'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.

³⁰ "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 July 2, 2024).

4. The Proposal's request for an external report would not micromanage Microchip's internal business operations but would assess and communicate to fellow shareholders to what extent Microchip's due diligence processes are aligned with evolving industry practice, rapidly evolving regulations, and the company's own Human Rights Policy and Guiding Values.

The filers' proposal does not micromanage Microchip's business or interfere with business operations. Rather it encourages the Company to conduct a level of KYC, human rights, and regulatory compliance due diligence that addresses the heightened risks to our Company through product misuse by Russia, Iran, and other bad actors operating in an increasing number of geopolitical conflicts. Additionally, Filers' proposal seeks to align Microchip's due diligence processes with industry standards and peers' best practices. The proposal seeks non-proprietary information at a reasonable expense and requests that a third party conducts the review to ensure an objective, expert opinion.

CONCLUSION

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,³¹ Myanmar,³² and Xinjiang Autonomous Region, China.³³ 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 U.S. Sustainable, Responsible and Impact Investing Trends.³⁴ 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 investors' long-term best interests and is not only compatible with but required by Microchip's stated "Guiding Values," specifically the commitment to responsible business practices, a long-term "ownership" perspective, and products and operations of which our Company can be proud.

³¹ "Investor Statement on the Crisis in Ukraine," Business & Human Rights Resource Centre, May 16, 2022, https://media.businesshumanrights.org/media/documents/Investor_Statement_on_the_Crisis_in_Ukraine_16_May_2022.pdf (accessed July 2, 2024).

³² "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 July 2, 2024).

³³ "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 July 2, 2024).

³⁴ "Report on US Sustainable, Responsible and Impact Investing Trends," US SIF Foundation, 2022 <https://www.ussif.org/Files/Trends/2022/Institutional%20Investors%202022.pdf> (accessed on July 2, 2024).

We urge you to vote FOR the Proposal requesting an independent third-party report on Microchip's due diligence process to determine whether customers' use of the Company's products contribute or are linked to violations of international law.

Sincerely,

Katie Carter
Director of Faith-Based Investing and Shareholder Engagement
Office of Faith-Based Investing and Shareholder Engagement
Presbyterian Church (U.S.A)

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, EMAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY. THE COST OF DISSEMINATING THE FOREGOING INFORMATION TO SHAREHOLDERS IS BEING BORNE ENTIRELY BY ONE OR MORE OF THE CO-FILERS. PROXY CARDS WILL NOT BE ACCEPTED BY ANY CO-FILER. PLEASE DO NOT SEND YOUR PROXY TO ANY CO-FILER. TO VOTE YOUR PROXY, PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.