UNITED STATES BANKRUPTCY COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

In re:	Chapter 11
23ANDME HOLDING CO., et al.,	Case No. 25-40976
Debtors.	(Jointly Administered)

THE UNITED STATES OF AMERICA'S NOTICE REGARDING POTENTIAL NATIONAL SECURITY CONCERNS

The United States of America submits this notice to inform the Court that one or more transactions contemplated by the Debtors may be subject to review by the Committee on Foreign Investment in the United States ("CFIUS") and may be prohibited or restricted by the Data Security Program administered by the Department of Justice, *see* 28 C.F.R. pt. 202. Bankruptcy courts have previously acknowledged that potential national security concerns (including CFIUS review) are relevant factors in bankruptcy proceedings, including specifically in determining whether bidders are qualified.[1]

[1] *See In re Enstrom Helicopter Corp.*, No. 22-90006 (SWD), ECF No. 33 (Bankr. W.D. Mich. Feb. 9, 2022) (letter from the Court to the parties: "It occurs to me that the sale may raise national security concerns, for example as a covered transaction within the purview of the Committee on Foreign Investment in the United States or similar authority. At the hearing, I will expect some assurance that you have considered the possibility and, if it is an issue in this case, you will be prepared to address it in a way that balances the government's interest in such matters and the estate's interest in an expeditious and unassailable sale." (citation omitted)); *id.* ECF No. 54-1 (Feb. 16, 2022) (court-approved bidding procedures include requirement to submit "information sufficient in the [Chapter 7] Trustee's judgment to determine whether a sale of the Assets to the Potential Bidder: (xx) will be a covered transaction or be subject to any mandatory declaration or other filing with any Governmental Body; and (yy) whether Potential Bidder is a foreign person for purposed of CFIUS or any other Law or regulation").

I. CFIUS Procedures and Review

A. Background

1. CFIUS is an interagency committee authorized to review certain transactions involving foreign investment in the United States ("covered transactions") to determine whether those transactions pose national security risks and, when appropriate, to mitigate the risks arising from those transactions, and to refer transactions to the President requesting his decision on whether to take an action to suspend or prohibit the transaction. *See* 50 U.S.C. § 4565(b)(1)(A), (*l*). Covered transactions include certain transactions that could arise pursuant to a bankruptcy proceeding. *Id.* § 4565(a)(4)(F); 31 C.F.R. § 800.213 note.

2. Section 721 of the Defense Production Act of 1950, as amended (codified at 50 U.S.C. § 4565), authorizes the President, acting through CFIUS, to review five types of covered transactions. 50 U.S.C. § 4565(a)(4)(B). A covered transaction could include the acquisition by a foreign national, foreign entity, or foreign government of a U.S. business that is in bankruptcy, including components of a business or assets that constitute a U.S. business under the CFIUS regulations. *See* 31 C.F.R. §§ 800.220 (defining a "foreign entity"); 800.223 (defining a "foreign national"); 800.224 (defining a "foreign person," which includes any entity that is controlled by a foreign national or foreign entity).

B. Procedure

3. Parties to a covered transaction may opt to voluntarily notify the transaction to CFIUS through a written notice or an abbreviated filing known as a declaration. Section 721 provides that certain transactions ***must*** be notified to CFIUS through a declaration submitted at least 30 days prior to a transaction closing. That requirement applies, for example, to certain covered transactions where a foreign government has a substantial interest. 50 U.S.C. § 4565(b)(1)(C)(v)(IV)(bb)(AA).

4. When a transaction comes before CFIUS, CFIUS completes a review to determine the transaction's potential impact on the national security of the United States. *Id.* § 4565(b)(1)(A), (F). Following this 45-day review period, two principal outcomes are possible. First, CFIUS may conclude action with respect to the transaction. *See* 31 C.F.R. § 800.506. Alternatively, if the review brings to light possible risks to U.S. national security, or if CFIUS needs more time to examine possible risks, CFIUS may initiate an investigation of up to 45 days into the "effects of [the] covered transaction on the national security of the United States." 50 U.S.C. § 4565(b)(2)(A), (C).

5. Upon completion of any investigation, CFIUS may conclude action with respect to the transaction, *see* 31 C.F.R. § 800.508(d), or send a report to the President requesting his decision on whether to take an action to suspend or prohibit the transaction, 50 U.S.C. § 4565(d)(1). When CFIUS sends a report to the President, the President has 15 days to decide whether to take action to suspend or prohibit the transaction. *Id.* § 4565(d)(2). The President's decision is not subject to judicial review. *Id.* § 4565(e).

6. CFIUS may seek to mitigate any threat to the national security of the United States that arises as a result of a covered transaction by entering into agreements with a party to the transaction or imposing conditions on the transaction. *See id.* § 4565(*l*)(3)(A).

C. Analysis

7. In determining whether to suspend a transaction, refer a transaction to the President, or require mitigation, CFIUS must undertake a risk-based analysis that includes assessment of the potential threat associated with the foreign acquirer based on its capabilities and intentions, vulnerabilities of the U.S. business, and consequences to national security if those vulnerabilities were to be exploited. *Id.* § 4565(*l*)(4)(A); 31 C.F.R. § 800.102 (defining "threat,"

"vulnerabilities," and "consequences to national security").

8. In conducting its national security risk analysis, CFIUS considers issues including "whether foreign investments in United States businesses that have access to or that store United States persons' sensitive data, including health and biological data, involve a foreign person who might take actions that threaten to impair" national security as a result of the transaction. Exec. Order No. 14083, 87 Fed. Reg. 57369, 57373 (Sept. 20, 2022).

D. Confidentiality

9. With limited exceptions, all information submitted to CFIUS is treated as confidential. *See* 50 U.S.C. § 4565(c)(1) ("any information or documentary material filed with the President or the President's designee [that is, CFIUS,] pursuant to this section shall be exempt from disclosure under [the Freedom of Information Act], and no such information or documentary material may be made public."). The limited exceptions to the confidentiality obligation include, for example, disclosure as may be relevant to any administrative or judicial action or proceeding. *See id.* § 4565(c).

10. Unauthorized disclosure of certain information or material filed with CFIUS can result in criminal penalties, including fines and imprisonment. *See* 31 C.F.R. § 800.802. "[T]here is . . . a clearly articulated intention, on the part of each of the legislative and executive branches of our government, that the CFIUS process remain confidential." *In re Glob. Crossing Ltd.*, 295 B.R. 720, 724-25 (Bankr. S.D.N.Y. 2003). The CFIUS statutory and regulatory confidentiality provisions apply in bankruptcy. *See id.* Nothing in the CFIUS confidentiality provisions, however, prohibits the public disclosure by a party of documentary material or information that the party itself has filed with CFIUS. *See* 31 C.F.R. § 800.802(d).

II. The Data Security Program Prohibits and Restricts U.S. Persons from Conducting Certain Commercial Transactions.

A. Background

20. Under Executive Order 14117, the U.S. Department of Justice administers a national-security program akin to sanctions or export controls that prevents certain countries of concern (including China, Russia, and Iran) and covered persons from leveraging commercial activities or relationships to access and exploit the sensitive personal data of U.S. persons. Exec. Order No. 14117, 89 Fed. Reg. 15,421 (Mar. 1, 2024); 28 C.F.R. pt. 202. Executive Order 14117 and the Data Security Program aim to address the "wide range of malicious activities" that countries of concern can engage in when they have access to sensitive personal data of U.S. persons, including "malicious cyber-enabled activities and malign foreign influence activities," and "track[ing] and build[ing] profiles on U.S. individuals, including members of the military and other Federal employees and contractors, for illicit purposes such as blackmail and espionage." Exec. Order No. 14117 at 15421; 90 Fed. Reg. at 1637.

21. To address the threats identified in Executive Order 14117, the Data Security Program prohibits or restricts certain commercial transactions between U.S. persons and "countries of concern" or "covered persons" where the transactions provide the countries of concern or covered persons the ability to access "sensitive personal data" on or above certain amounts of U.S. persons. *See* 28 C.F.R. § 202.249 (defining the term "sensitive personal data" as "covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data," including human genomic data, "personal health data, personal financial data, or any combination thereof.").

22. As explained in greater detail below, the Data Security Program's prohibitions and restrictions may be triggered by bankruptcy proceedings in which a debtor has U.S. sensitive

personal data if, for example, the debtor is proposing a sale of data to, or investment, employment, or vendor arrangements with, countries of concern or covered persons.

B. Countries of Concern and Covered Persons

23. The data security regulations identify China, Cuba, Iran, North Korea, Russia and Venezuela as "countries of concern." *Id*. § 202.601. They also define "covered persons" as foreign entities that are "organized or chartered under the laws" of a country of concern, have their "principal place of business" in a country of concern, or are "50% or more owned" by a country of concern or another covered person, and as foreign individuals who are employed or contracted by a country of concern or covered person, or who "primarily reside" in a country of concern. *Id*. § 202.211. (defining "covered persons"). For example, a company with its principal place of business in China, and an individual who primarily resides in Russia, are both covered persons.

C. Prohibited Transactions

24. The Data Security Program prohibits, *inter alia*, U.S. entities and individuals from knowingly engaging in certain commercial transactions that provide covered persons or countries of concern the ability to access "human genomic data" and "human biospecimens from which human genomic data can be derived" on more than 100 U.S. persons. *See id*. § 202.303 (prohibiting certain "human 'omic data and human biospecimen transactions"); *id.* § 202.244(1) (defining "human genomic data"); *id*. § 202.223 (defining "human biospecimens"); *id*. § 202.205 (setting a numerical threshold triggering the Data Security Program's applicability for human genomic data transactions at "more than 100 U.S. persons"). This prohibition prevents U.S. businesses from providing countries of concern or covered persons with the ability to access human genomic data through commercial transactions, including through "data brokerage"—selling the data, licensing access to the data, or conducting other similar commercial transactions, as well as through

investments agreements, employment agreements and vendor agreements. *See id*. § 202.210 (defining the commercial transactions covered by the Data Security Program as "covered data transactions" that include "data brokerage," "vendor agreement[s]," "employment agreement[s]" and "investment agreement[s]"); *id*. at § 202.214 (defining "data brokerage"); *id*. § 202.228 (defining an "investment agreement"); *id*. § 202.217 (defining an "employment agreement"); *id*. § 202.258 (defining a "vendor agreement").

25. The Data Security Program also prohibits "data brokerage" transactions that provide countries of concern or covered persons the ability to access other types of sensitive personal data beyond human genomic data and human biospecimens, including "biometric identifiers," such as fingerprints, on more than 1,000 U.S. persons, "precise geolocation data," on more than 1,000 U.S. devices, "personal health data," on more than 10,000 U.S. persons, and "covered personal identifiers," such as Internet Protocol addresses or internet cookies when coupled with other covered identifiers, on more than 100,000 U.S. persons. *Id*. § 202.204 (defining "biometric identifiers); id. § 202.242 (defining "personal geolocation data"); *id*. § 202.241 (defining "personal health data"); *id.* § 202.212 (defining "covered personal identifiers"); *id*. § 202.205 (setting the numerical thresholds triggering the Data Security Programs' applicability).

D. Restricted Transactions

25. In addition to prohibitions, the Data Security Program restricts three categories of commercial transactions (investment agreements, employment agreements, and vendor agreements) that provide countries of concern or covered persons the ability to access sensitive personal data that is not human genomic data or human biospecimens on certain amounts of U.S. persons. United States persons undertaking such transactions must implement "security requirements" to, *inter alia*, restrict covered person and country of concern access to the data. *Id*.

§ 202.401) (providing authorization to conduct "restricted transactions"); *id*. § 202.248 (defining the term "security requirements").

E. Obligations of U.S. Businesses

26. A U.S. business must comply with the Data Security Program's prohibitions and restrictions, which include prohibiting the U.S. business from knowingly selling the sensitive personal data—including the human genomic data—that it has collected or that it maintains on U.S. persons to certain buyers. For example, the Data Security Program prohibits a U.S. business from selling the human genomic data it maintains on more than 100 U.S. persons to a company that is 50% or more owned by a company headquartered in a country of concern, such as China. Likewise, the Data Security Program prohibits a U.S. business from obtaining investments from an individual who lives primarily in a country of concern, such as Russia, where the investor obtains the ability to access the human genomic data the U.S. business maintains on more than 100 U.S. persons. U.S. businesses must comply with the Data Security Program's prohibitions and restrictions even when the data they maintain is already encrypted, anonymized, aggregated or de-identified. *Id*. § 202.206.

F. Penalties

27. The National Security Division of the Department of Justice oversees the Data Security Program and has an interest in ensuring that United States persons comply with its provisions as part of its mission to protect the United States from threats to U.S. national security. The International Emergency Economic Powers Act ("IEEPA") and the Data Security Program authorize the Department of Justice to bring civil and criminal enforcement actions for knowing or, with respect to only criminal enforcement, willful violations of the data security regulations. 50 U.S.C. 1705; 28 C.F.R. § 202.1301.

Dated: April 17, 2025

Respectfully submitted,

SAYLER A. FLEMING
United States Attorney

/s/ *Joshua M. Jones*
JOSHUA M. JONES #61988MO
Assistant United States Attorney
Thomas F. Eagleton U.S. Courthouse
111 South Tenth Street, 20th Floor
St. Louis, Missouri 63102
(314) 539-2310
(314) 539-2287 fax
joshua.m.jones@usdoj.gov

Certificate of Service

Pursuant to L.R. 9004(D), the undersigned hereby certifies that on April 17, 2025, the foregoing was filed electronically and therefore served by operation of the Court's CM/ECF system upon all parties in interest participating in said system.

The undersigned hereby certifies that on April 17, 2025, that all parties identified in this Court's "Interim Order (I) Establishing Certain Notice, Case Management, and Administrative Procedures and (II) Granting Related Relief," *see* doc. 131 at ¶ 6, were served a copy of the foregoing via electronic mail or United States mail, postage prepaid, utilizing the Master Service List appended hereto as Exhibit A.

/s/ *Joshua M. Jones*
Assistant United States Attorney