INVESTMENT COMPANY INSTITUTE

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

March 18, 2014

Mr. John Hounsell
National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Re: Certification Program for Access
To the Death Master File (DMF)

Dear Mr. Hounsell:

The Investment Company Institute (the "Institute")[1] appreciates the opportunity to provide its comments to the National Technical Information Service within the U.S. Department of Commerce in connection with its Request for Information and Advance Notice of Public Meeting (the "Notice") regarding the establishment and implementation of a certification program for access to the Death Master File ("DMF").[2] The stated purpose of the Notice is to solicit information necessary to assist the Secretary of Commerce in implementing the requirement in Section 203 of the Bipartisan Budget Act of 2013, which requires the Secretary to establish a program to limit access to the DMF to certified persons. The Institute has a significant interest in sharing our comments regarding this matter inasmuch as our members, which are mutual funds[3], are long-time users of the DMF and continued access to it remains of great importance to them.

---

[1] The Investment Company Institute is the national association of U.S. investment companies, including mutual funds, closed-end funds, exchange-traded funds (ETFs), and unit investment trusts (UITs). ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers. Members of ICI manage total assets of $16.3 trillion and serve more than 90 million shareholders.

[2] *See Certification Program for Access to the Death Master File,* Department of Commerce Docket No. 140205103-4103-01; RIN 0692-AA21 (February 25, 2014) (the "Notice").

[3] As used in this letter, the term "mutual fund" refers to the mutual fund complex. Unlike other companies, a mutual fund is typically externally managed. As such, it relies upon third parties or service providers – either affiliated organizations or independent contractors – to invest fund assets, maintain shareholder records, and carry out other business activities. The primary types of service providers relied upon by a mutual fund to carry out its business include, among others, an investment adviser, transfer agent, custodian, and principal underwriter. When the mutual fund's service providers perform services on behalf of the mutual fund, they do so pursuant to an agreement with the fund that, in part, requires them to fulfill the fund's compliance obligations with regulatory requirements, including the requirements discussed in this letter.

The Notice acknowledges the importance of the DMF in assisting the financial community, insurance companies, and state and local governments in identifying and preventing identity fraud, and identifying customers who are deceased. It raises a variety of questions designed to further inform the Secretary on how such institutions utilize the DMF, including any legal requirements to do so, and how they protect the confidentiality of information obtained from the DMF. As discussed in more detail below, mutual funds routinely rely on information contained in the DMF to fulfill their regulatory responsibilities under federal law to protect mutual funds shareholders and to prevent or mitigate fraudulent conduct, including identity theft, money laundering and the funding of terrorist activities through such illegal activities. Mutual funds are also subject to very rigorous data protection and security requirements and thus have considerable experience in maintaining the confidentiality, security, and appropriate use of information obtained from the DMF.

I. BACKGROUND

As noted above, this letter is being filed on behalf of members of the Investment Company Institute. Members of the Institute are registered investment companies – more commonly known as mutual funds. Mutual funds are subject to a strict regime of regulation under the federal securities laws. These laws include, among others, the Investment Company Act of 1940 (the "ICA"), the Investment Advisers Act of 1940, the Securities Exchange Act of 1934 ("Securities Exchange Act"), and the Securities Act of 1933, as well as rules of the U.S. Securities and Exchange Commission ("SEC") and the self-regulatory organizations (*e.g.,* Financial Institution Regulatory Authority ("FINRA")) adopted under such laws. In addition, they are subject to additional federal laws applicable to financial institutions (which term, for certain purposes, includes mutual funds). These laws include, for example, the Bank Secrecy Act ("BSA"), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), and the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd Frank Act"). They are also subject to certain regulations adopted under these statutes such as the regulations imposed on financial institutions by the Financial Crimes Enforcement Network ("FinCEN")). To ensure their compliance with all such requirements, mutual funds are also subject to inspections conducted by the staff of the SEC.

II. MUTUAL FUND USE OF THE DMF

As mentioned above, mutual funds routinely rely on information obtained from the DMF to fulfill their regulatory responsibilities. General speaking, there are at least three federal laws that necessitate mutual funds' use of the DMF: *i.e.,* the USA PATRIOT Act, the Dodd-Frank Act, and the Securities Exchange Act. The obligations imposed by these laws on mutual funds that necessitate mutual funds' use of the DMF are described in more detail below.

A. The USA PATRIOT Act

The USA PATRIOT Act was enacted by Congress in 2001 in response to the September 11, 2001 terrorist attacks. In part, the USA PATRIOT Act revised Sections 326 and 352 of the BSA in an effort to make it easier to prevent, detect, and prosecute money laundering and the financing of terrorism. Consistent with this goal, Section 326 of the USA PATRIOT Act amended the BSA to require financial institutions – which term includes mutual funds – to establish written customer identification programs ("CIPs"). To implement this requirement, in 2003 the SEC and FinCEN jointly adopted rules that impose CIP obligations on mutual funds.[4] Pursuant to these rules, mutual funds are required to implement procedures to: verify the identity of any person seeking to open an account, to the extent reasonable and practicable; maintain records of the information used to verify the person's identity; and determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations. At a minimum, the rules require mutual funds to obtain the shareholder's name, date of birth, address, and certain identification numbers, including the individual's social security number, and to have and implement written procedures to verify the customer's identity. The rules also include provisions governing the use of documentary and non-documentary methods that funds may use to verify the customer's identity. According to SEC Rule 103.131(b)(2)(ii)(B)(1), the non-documentary methods may include "information obtained from a consumer reporting agency, public database, or other source."

Of particular significance for purposes of the Notice, in fulfilling their verification responsibilities under their CIPs, mutual funds often utilize information from the DMF to ensure that a person opening a new account is not, in fact, using the identity of a deceased person.

Section 352 of the USA PATRIOT Act also impacted mutual funds. This section amended the BSA to require financial institutions, which the BSA defines to include mutual funds, to develop and implement anti-money laundering ("AML") compliance programs. To implement this requirement, FinCEN adopted a rule that, in part, requires mutual funds to establish AML compliance programs.[5] The rule further requires each mutual fund identify its vulnerabilities, understand applicable BSA requirements, identify its risks factors, design procedures and controls that will reasonably assure compliance with the AML requirements, and periodically assess the effectiveness of such procedures and controls. A mutual fund's AML compliance program must be in writing, it must be approved by the fund's board of directors, and, at a minimum, it must include, among other things, policies, procedures, and internal controls that are reasonably designed to prevent the mutual fund from being used for money laundering or the financing of terrorist activities. The program must also achieve compliance with the BSA and the implementing rules and provide for the designation of a person or

---

[4] *See* 31 C.F.R. § 1024.220.

[5] *See* 31 C.F.R. § 1024.210.

persons responsible for implementing and monitoring the operations and internal controls of the AML program – *i.e.,* an AML Officer.

Of particular significance for purposes of the Notice, in fulfilling the AML requirements, particularly those designed to address money laundering concerns, mutual funds often utilize information from the DMF to ensure that shareholders are not using the identity of a deceased person.

B. The Dodd-Frank Act

Section 1088 of the Dodd-Frank Act amended the Fair Credit Reporting Act to require the SEC to adopt and enforce rules and guidelines regarding the detection, prevention, and mitigation of identity theft. These rules, known as the "identity theft red flag rules," apply to all entities subject to the SEC's enforcement jurisdiction.[6] In April 2013, the SEC adopted the required rules.[7] As noted in the SEC Release adopting them, the rules further the interest of the federal government in taking steps to help protect individuals from the risk of theft, loss, and abuse of their personal information – including the risks associated with identify theft. The rules require mutual funds to establish and oversee a program that is designed to detect, prevent, and mitigate identify theft in connection with shareholders' accounts. Among other things, a mutual fund's program must include reasonable policies and procedure to identify, detect, and respond to red flags and it must be updated periodically to reflect changes in risks to customers and to the institution from identity theft. The rules include extensive guidance to assist SEC registrants in implementing, operating, and overseeing their programs on an on-going basis. As noted by information available on the website of the Identity Theft Resource Center, it is not uncommon for identity thieves to fraudulently use the Social Security Number of a deceased person to pose as such person for the thief's own personal gain.[8] Mutual funds routinely rely on information in the DMF to implement their identity theft red flag programs and to protect their shareholders from thieves who attempt to steal the identity of a deceased shareholder before the mutual fund knows of the shareholder's death.

---

[6] Prior to the enactment of the Dodd-Frank Act, mutual funds had been subject to identity theft red flag rules that had been adopted by the Federal Trade Commission pursuant to 2003 amendments to the Fair Credit Reporting Act. The Dodd-Frank Act transferred the rulemaking and enforcement jurisdiction for the identity theft red flag rules from the FTC to the SEC with respect to SEC registrants. The rules adopted by the SEC pursuant to the Dodd-Frank Act are substantively identical to those of the FTC.

[7] *See Identity Theft Red Flag Rules,* SEC Release No. IC-30452 (April 10, 2013).

[8] *See* www.idtheftcenter.org.

C. The Securities Exchange Act

All mutual funds rely on the services of a transfer agent to maintain shareholder records for the mutual fund. These transfer agents are registered and strictly regulated by the SEC under Section 17A of the Securities Exchange Act. Rules adopted by the SEC under this statutory section require mutual funds to report any "lost securityholder" to the SEC. Generally speaking, a lost securityholder is a person who has either abandoned or forgotten about an account, or a shareholder who has died without such person's relatives notifying the mutual fund's transfer agent to arrange for the appropriate disposition of the account.[9]

Pursuant to SEC Rule 17Ad-17, a mutual fund's transfer agent is required by law to search for any lost securityholder. In particular, the rule requires the transfer agent to "conduct two data base searches using at least one information data base service" and to "search by taxpayer identification number or by name if a search based on taxpayer identification number is not reasonably likely to locate the securityholder."[10]

Importantly, in conducting the required searches, mutual fund transfer agents utilize the DMF to determine whether the shareholder is deceased. The mutual fund transfer agent must keep a record of its searches and their results and include such information in an annual report the transfer agent is required to file with the SEC. If the mutual fund's transfer agent determines that the accountholder is deceased, it attempts to locate either the decedent's authorized representative or beneficiaries in order to make arrangements for disposition of the shareholder's account.

In addition to searching for and reporting lost securityholder information to the SEC, mutual funds are also required to escheat unclaimed accounts to the state of residence of the accountholder. Every state has an unclaimed property law that requires holders of unclaimed property to turn such property over to the state once a specified dormancy period has passed. Depending on the state, these dormancy periods are typically 3-7 years following a specified triggering event. Most states' triggering events are either the same returned mail standard set forth in SEC Rule 17Ad-17 or the shareholder's lack of contact with the holder (*i.e.,* the mutual fund's transfer agent, which maintains customer account records on behalf of the mutual fund). Regardless of the triggering event, once the event occurs and the dormancy period passes, unless the mutual fund is able to locate the shareholder, the shareholder's property must be turned over to a state for disposition. Mutual funds are diligent about

---

[9] SEC Rule 17Ad-17(b)(2) under the Securities Exchange Act defines a "lost securityholder" as a securityholder "to whom an item of correspondence that was sent to the securityholder at the address contained in the transfer agent's master securityholder file has been returned as undeliverable; providing however, that if such item is re-sent within one month to the lost securityholder, the transfer agent may deem the securityholder to be a lost securityholder as of the day the recent item is returned as undeliverable."

[10] *See* SEC Rule 17Ad-17(a)(1) under the Securities Exchange Act.

trying to locate lost shareholders to avoid having to escheat the shareholder's property to the states.[11] They routinely rely on the DMF to assist them in this process.

III. PRIVACY PROTECTIONS

Title V of the Gramm-Leach Bliley Act required federal regulators of financial institutions to adopt regulations to govern the use of consumers' non-public personal information.[12] For purposes of the Act, the SEC is considered a federal regulator of financial institutions and the term "financial institution" includes mutual funds. In response to the Gramm-Leach-Bliley Act, the SEC adopted Regulation S-P.[13] Among other things, Regulation S-P requires mutual funds to: protect the privacy of shareholders' non-public personal information; limit the ability of mutual funds to share such nonpublic personal information; and adopt policies and procedures that are reasonably designed to ensure the security, confidentiality, and integrity of customer records and to protect them against hazards and unauthorized access. With respect to the sharing of a shareholder's non-public personal information, Regulation S-P prohibits such sharing unless it falls within one of the permitted purposes set forth in the regulation or is expressly consented to by the shareholder. Permissible sharing purposes include, for example, sharing that is necessary: to process and service a transaction requested by the customer; to prevent fraud, unauthorized transactions, claims, or other liability; for required institutional risk control or to resolve consumer disputes; and to comply with applicable law, or regulatory, legal, or judicial process.[14] Importantly, Regulation S-P also prohibits a mutual fund from sharing or disclosing any non-public personal information to a nonaffiliated third party unless the third party agrees to preserve the confidentiality of the information in accordance with Regulation S-P. Also, if the mutual fund receives confidential information on a shareholder from a nonaffiliated financial institution, the fund, too, must agree to preserve the confidentiality of such information as required by Regulation S-P.

Inasmuch as investors' confidence in the securities markets depends, in part, on the protection of their confidential account information, our members take their privacy responsibilities very seriously. Over the years, they have spent hundreds of millions of dollars to build and keep current their systems

---

[11] Mutual funds, on behalf of their shareholders, have an interest in protecting shareholders' accounts from escheating to the states because, in many states, once the property escheats, the account is liquidated and the liquidated proceeds are held by the state on behalf of the accountholder. While the accountholder can reclaim the property, they only receive the proceeds from the liquidation and not any gains or appreciation on them. Moreover, to the extent the account was a tax-advantaged account (*e.g.,* a 401(k) retirement account or a 529 education savings account), the shareholder may incur significant tax penalties as a result of the state's liquidation of the account.

[12] *See* Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[13] *See Privacy of Consumer Financial Information (Regulation S-P),* SEC Release No. IC-24543 (June 22, 2000).

[14] *See* §248.15 of Regulation S-P.

to protect shareholder data, and they are diligent about staying informed of new and emerging threats to shareholders.

Importantly, any information on shareholders mutual funds obtain from DMF is protected to the same extent as other non-public personal information they obtain from or maintain on behalf of their shareholders.

It should also be noted that, pursuant to SEC Rule 38a-1 under the Investment Company Act, the compliance policies, procedures, and processes mutual funds have in place to fulfill their regulatory responsibilities are not – and cannot be – static. Instead, Rule 38a-1 requires mutual funds to: adopt compliance policies and procedures that are reasonably designed to ensure the fund's compliance with the federal securities laws as well as with the BSA; have such policies and procedures approved by the fund's board of directors; appoint a chief compliance officer to oversee implementation of the policies and procedures on an ongoing basis; annually test such policies and procedures for their adequacy and the effectiveness of their implementation; and provide an annual written report to the fund's board that, among other things, includes the results of the annual testing and any changes made to the policies and procedures to address material compliance matters. As a result of Rule 38a-1, mutual funds are required by law to keep their policies and procedures current and to continually assess their effectiveness and implementation.

IV. THE INSTITUTE'S RESPONSE TO THE QUESTIONS RAISED IN THE NOTICE

Against the backdrop of the above information regarding how mutual funds utilize information in the DMF to fulfill their regulatory responsibilities and the systems and procedures that are in place to protect shareholders' non-public personal information, the Institute's response to the questions raised in the Notice are as follows:

A. Certification Program

1. Do mutual funds have a legitimate fraud interest in accessing the DMF? If so, explain the basis of that interest.

   Institute Response: As discussed above, mutual funds have a legitimate fraud interest in checking the information available in the DMF as part of their CIP, AML, and red flag programs, to protect against identity theft and other fraudulent conduct, and to verify whether a lost securityholder is deceased. Such information is used by mutual funds, not only to protect their customers, *i.e.*, mutual funds shareholders, but also to serve important public policy purposes.

2-5. If mutual funds have a legitimate business purpose to access the DMF pursuant to law, rule, regulation, or fiduciary duty, explain in detail and cite the relevant law/rule/regulation/fiduciary duty.

Institute Response: As discussed in detail above, provisions in the USA PATRIOT Act, the Dodd-Frank Act, and the Securities Exchange Act as well as rules of the SEC under these Acts necessitate mutual fund's use of the DMF for legitimate business purposes.

6. Do mutual funds have systems, facilities, and procedures in place to safeguard DMF information and experience in maintaining the confidentiality, security, and appropriate use of such information?

Institute Response: Yes. As discussed above, mutual funds are subject to very rigorous data protection and security requirements under the Gramm-Leach-Bliley Act and SEC Regulation S-P. Also, mutual funds have long utilized information in the DMF to fulfill their regulatory responsibilities and thus have considerable experience in maintaining the confidentiality, security, and appropriate use of such information.

7. If your answer to Question 6 is "yes," explain whether and how your systems, facilities, and procedures are audited, inspected, or monitored?

Institute Response: As discussed above, mutual funds have an affirmative legal responsibility to maintain compliance policies and procedures that are reasonably designed to ensure their compliance with all applicable regulatory requirements under the federal securities laws and the BSA.[15] Rule 38a-1 under the Investment Company Act requires mutual funds to annually test the adequacy of their policies and procedures and the effectiveness of their implementation and provide a written report to the fund's board regarding such testing as well as information on any material compliance matters.

8. Explain whether your response to Question 7 occurs on a voluntary basis or if it is required by law.

Institute Response: As noted in our response to Question 7, mutual funds are required by law to continually review their policies, procedures, and systems and report annually to the mutual fund's board regarding such reviews.

9. Explain whether any reviews discussed in response to Question 7 would reveal how a mutual fund uses DMF information, whether DMF information has been disclosed to a third person, and if so, how it was used or disclosed by such person.

---

[15] SEC Rule 38a-1 defines the term "Federal securities laws" to include the BSA. *See* SEC Rule 38a-1((e)(1).

Institute Response: As discussed above, SEC Regulation S-P imposes very rigorous requirements regarding a mutual fund's use of non-public personal information (which would include any information obtained from the DMF on a shareholder) and the sharing of such information. In addition, SEC Rule 38a-1 requires mutual funds to annually review their compliance with the SEC's regulatory requirements, which would include review of the issues raised by this question.

10. Explain in detail the extent to which mutual funds can satisfy requirements similar to the privacy protections in Section 6103(p)(4) of the Internal Revenue Code.

    Institute Response: Section 6103(p)(4) requires persons receiving tax returns or return information from the Internal Revenue Service ("IRS") to safeguard such information. It is not uncommon for mutual funds to receive sensitive information on shareholders from the IRS (*e.g.,* C-Notices (requiring the transfer agent to backup withhold reportable payments to the IRS on a shareholder that may be underreporting income to the IRS) and tax levies (on shareholders that owe money to the IRS)), including the shareholder's name, social security number, and address. Mutual funds protect such information to the same degree that they protect other non-public personal information held on shareholders as required by SEC Regulation S-P.

11. If you currently do not have systems in place to safeguard DMF information, explain how mutual funds anticipate putting such systems in place.

    Institute Response: As discussed above, mutual funds currently have systems in place to protect non-public personal information.

12. Explain how the safeguards mutual funds have in place to protect shareholders' non-public personal information are similar to the requirements of Section 6103(p)(4).

    Institute Response: See response to Question 10, above.

13. What system, facilities, and procedures are necessary to safeguard DMF information?

    Institute Response: With respect to mutual funds, we believe the protections afforded by SEC Regulation S-P under the GLB Act address each of the data security concerns that are necessary to safeguard DMF information.

14. Identify laws or regulations that require the safeguarding of released DMF information and summarize the procedures required by such laws or regulations.

Institute Response: See the discussion relating to the privacy provisions of SEC Regulation S-P and Rule 38a-1, which can be found at pages 6-7, above.

B. Fees and Penalties

15. Would the imposition of a single, presumably larger, fee at the time of certification be preferable to the charge of multiple, presumably smaller, fees, such as annual fees?

Institute Response: At this time there is not enough information regarding the intended application of a fee-based certification program to allow for a meaningful response to this question. For example, if one fee is charged at the time of certification, would that fee cover all future access to the DMF or is it possible that additional fees would be assessed in the future? How would such fee be determined? Would it be determined on: a pro-rata basis; on the basis of how frequently the entity plans to access the DMF; on the size of the entity accessing the DMF; on some other basis? If it will be assessed on a pro-rata basis, how will the fee be determined as the community of persons utilizing the DMF are likely to change from year to year? If a periodic (annual) charge is imposed, what factors will determine the size of that fee and when and how often it is assessed?

Until such time as we have more information regarding how the various fees might be assessed, we are unable to answer this question. As the Secretary considers how fees for accessing the DMF will be implemented, however, it is important to recognize that, as discussed above, mutual funds routinely rely on information provided by the DMF to fulfill their regulatory responsibilities under federal law to protect their shareholders through the prevention and mitigation of fraudulent conduct, including identity theft, money laundering and the funding of terrorist activities through such illegal activities. We therefore urge the Secretary to adopt a fee structure that is reasonable.

16. In order to become certified to have access to the DMF, how would mutual funds prevent disclosure of DMF information to any person not certified to receive the information?

Institute Response: Due to the sensitive nature of the non-public personal information that mutual funds have regarding their shareholders in the normal course of business, they currently have in place policies, procedures, processes, and systems to limit access to sensitive and non-public information – including information they currently receive from the DMF or the IRS – on a "needs to know" basis. Also, as noted above, because mutual funds rely upon the use of such information and mutual fund shareholders rely upon mutual funds to maintain the confidentiality of their personal account information, mutual funds take very seriously their obligation to do so under SEC Regulation S-P. Accordingly, limiting access to the DMF information to certified persons would not be problematic for mutual funds.

C. Death Master File Information

17. If mutual funds currently access DMF information, does their use of that information include or require the name, social security account number, date of birth, and date of death of deceased individuals? If not, explain the DMF information mutual funds do not use.

Institute Response: Mutual funds currently utilize all four pieces of information from the DMF. This is because information from the DMF is used to verify information obtained from shareholders in order to fulfill the panoply of their regulatory responsibilities. For example, in trying to locate lost securityholders, it is important that mutual funds be provided access to as much information as possible to verify whether the name, social security number, and date of birth on the mutual fund's records match those on file with the DMF. The shareholder's date of death is also relevant to the mutual fund to assist it in locating potential beneficiaries on the account and their associated status at the time of the shareholder's death.

18. Would mutual funds find it useful to access DMF information that did not include one or more of the following pieces of information: name, social security number, date of birth, and date of death of a deceased individual?

Institute Response: For the reasons discussed above, and for the purposes for which mutual funds access the DMF, it is crucial that we continue to have access to all information currently available through the DMF.

▪ ▪ ▪ ▪ ▪

We appreciate the opportunity to provide these comments and we hope you find them useful as the Secretary implements the provisions of the Bipartisan Budget Act of 2013 relating to the DMF. If you have any questions regarding the mutual fund industry or the importance to mutual funds of ensuring continued access to the DMF in order to meet their substantial and comprehensive regulatory obligations, please contact the undersigned at (202)326-5825.

Sincerely,
/s/
Tamara K. Salmon
Senior Associate Counsel