



FINANCIAL
SERVICES
ROUNDTABLE

Via e-mail to jhounsell@ntis.gov

March 30, 2015

Bruce Borzino
Director
National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

**RE: CERTIFICATION PROGRAM FOR ACCESS TO THE DEATH MASTER FILE
[DOCKET No. 141219001-4999-02]**

Dear Director Borzino:

The Financial Services Roundtable (“FSR”)¹ and BITS² hereby submit the following comments on the proposed final rule issued by the National Technical Information Service (“NTIS”) and published in the Federal Register on December 30, 2014, regarding the establishment of a certification program for access to the Social

¹ As advocates for a strong financial future™, FSR represents the largest integrated financial services companies providing banking, insurance, payment, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America’s economic engine, accounting directly for \$92.7 trillion in managed assets, \$1.2 trillion in revenue, and 2.3 million jobs.

² BITS is the technology policy division of FSR. BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services.

Security Administration’s Death Master File (“DMF”), pursuant to Section 203 of the Bipartisan Budget Act of 2013 (the “Proposed Final Rule”).³

1. EXECUTIVE SUMMARY

- We urge NTIS to clarify that the use of DMF data to facilitate payment to beneficiaries is a “legitimate business purpose” within the meaning of Section 203.
- NTIS should further clarify that third-party vendors that assist financial services firms in the performance of anti-fraud functions are deemed to “have” a legitimate fraud prevention interest within the meaning of section 203.
- We urge NTIS to adopt a final rule that expressly provides that communications with beneficiaries (“Beneficiary Communications”) regarding the fact of death—which does not entail disclosure of the deceased’s social security number—does not implicate the certification requirement. This revision, which would ensure that firms may engage in Beneficiary Communications, is essential because the laws of fifteen (15) states now require certain financial services companies to search the DMF to identify deceased policyholders for the purpose of facilitating payment to beneficiaries, and similar legislation is under consideration in other states. Many companies also undertake DMF searches as a pro-consumer practice or pursuant to regulatory settlement agreements. Therefore, NTIS should ensure that the final rule would not preclude companies from engaging in Beneficiary Communications concerning entitlement to benefits, which provide necessary services for consumers, or assists companies in meeting their obligations under applicable state laws.
- The proposed data security protections for DMF data (including audit requirements) that would be imposed on financial services companies, which are already required by the Gramm-Leach-Bliley Act (“GLBA”) to safeguard their customers’ personal information, would risk undercutting the flexibility that is critical to combatting identity-related fraud and imposing additional operating burdens on these firms without any commensurate gain in data security.
- The GLBA’s data-security requirements, which were created specifically for financial institutions handling sensitive personal information, are an

³ Department of Commerce, National Technical Information Service, Temporary Certification Program for Access to the Death Master File (“Interim Final Rule”), 79 Fed. Reg. 16668 (Mar. 26, 2014).

appropriate yardstick for measuring the sufficiency of a firm's data-protection measures for purposes of DMF access.

- Because the GLBA's requirements are "similar" to those of section 6103(p)(4) of the Internal Revenue Code, compliance with the GLBA with respect to Limited Access DMF data would satisfy the proposed data-security certification requirements.
- We urge NTIS to adopt a final rule that expressly provides companies facing penalties and potential liabilities arising out of unscheduled audits and substantial financial penalties with procedural rights, including the rights of appeal to an administrative law judge and ultimately to federal court.

2. CERTIFICATION REQUIREMENT

The certification requirement in the Proposed Final Rule raises two issues of concern to our members. *First*, the Proposed Final Rule fails to address numerous questions raised in comment letters to NTIS regarding the type and scope of DMF access that qualifies as a "legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty." Financial services companies face particular uncertainty regarding pro-consumer usage of the DMF to promote prompt and accurate payment to beneficiaries, notwithstanding that the Request for Information originally issued by NTIS specifically identifies the "fulfillment of benefits to . . . beneficiaries" as an "important" use of DMF data. Certain companies are required to conduct such searches pursuant to regulatory settlement agreements, and fifteen states have recently passed laws requiring life insurance companies to search the DMF for the purpose of facilitating the payment of benefits.⁴ However, not all companies that conduct such searches in order to serve consumers are clearly required to do so "pursuant to a law, governmental rule, regulation or fiduciary duty." As a result, the Proposed Final Rule risks harming consumers by

⁴ See ALA. CODE § 27-15-52 (2014); 2013 Georgia House Bill No. 920, Georgia One Hundred Fifty-Second General Assembly - 2013- 2014 Regular Session; 2014 Indiana Senate Bill No. 220, Indiana One Hundred Eighteenth General Assembly - Second Regular Session (Indiana Unclaimed Life insurance Benefits Act, Pub. L. No. 90) (March 20, 2014); KY. REV. STAT. ANN. § 304.15-420 (2014); MD. CODE ANN., INS. § 16-118 (2014); 2014 Mississippi Senate Bill No. 2796, Mississippi One Hundred Twenty-Ninth Legislative Session (Mississippi Unclaimed Life Insurance Benefits Act) (March 24, 2014); MONT. CODE ANN. § 33-20-1604 (2014); NEV. REV. STAT. §§ 688d.090 (2014); N.M. STAT. § 59a-16-7.1 (2014); N.Y. INS. LAW § 3240 (2014); N.D. CENT. CODE §§ 26.1-55-01 to -05 (2014); 2013 Tennessee Senate Bill No. 2516, Tennessee One Hundred Eighth General Assembly - Second Regular Session; and VT. STAT. ANN. Tit. 27, § 1244a (2014).

restricting or creating uncertainty regarding financial services firms' ability to use the DMF to serve this important purpose. *Second*, it is unclear whether the Proposed Certification Form allows DMF access for third-party vendors to which many financial services companies outsource important fraud-prevention activities.

We urge NTIS to clarify that use of DMF data to facilitate payment to beneficiaries is a “legitimate business purpose” within the meaning of section 203, and that third-party vendors that assist financial services firms with DMF search functions (thereby providing critical support to financial services firms in the performance of anti-fraud functions), are deemed to “have” a legitimate fraud prevention interest within the meaning of section 203.

3. DISCLOSURE OF DMF DATA TO THIRD PARTIES

The Proposed Final Rule would require companies seeking DMF access to certify that they will not disclose DMF data to any person who is not certified for DMF access. As noted above, one of the legitimate business purposes for which financial services firms use the DMF is to determine whether benefits may be owed – for example, under a life insurance policy – and to notify the beneficiary, and certain states now require this type of DMF usage. We previously requested clarification that the rule was not intended to prevent financial services firms from communicating with beneficiaries about the fact of death, which is generally known to the beneficiary and may be publicly available in any event through published obituaries.

The present proposal to revise the definition of “Limited Access DMF” to clarify that an individual element of information obtained through a source independent of the Limited Access DMF “is not to be considered part of the Limited Access DMF if the NTIS source information is replaced with the newly provided information” is a step in the right direction but does not go far enough to permit financial services firms to communicate with beneficiaries in instances when the death is not reflected in an obituary or other publicly-available source. We urge NTIS to adopt a final rule that expressly provides that communications with beneficiaries regarding the fact of death, which does not entail disclosure of the deceased’s social security number, does not implicate the certification requirement. If financial services firms are precluded from communicating with beneficiaries regarding their entitlement to benefits, the certification process risks undermining rather than enhancing consumer rights and places financial services firms in the position of being required by certain state laws to conduct DMF searches yet prevented by federal law from fulfilling the purpose of those searches.

Finally, the proposed requirement that Limited Access DMF information be “replaced” by confirmatory public information seems unnecessary and potentially confusing. If the Limited Access DMF indicates that a particular individual’s date of death was June 30, 2014, and an obituary confirms that the date of death was June 30, 2014, it is not clear what it means to “replace” the DMF data on date of death with data

obtained from an obituary or what would be gained by doing that. As a result, we recommend that NTIS eliminate the “replacement requirement” from the final rule.

4. PROPOSED CERTIFICATION AND AUDIT REQUIREMENTS

The Proposed Final Rule would subject any entity seeking access to the Limited Access DMF to (i) submit a written attestation from an independent Accredited Certification Body that such person has information security systems, facilities, and procedures in place to protect the security of the DMF information, and (ii) submit to “periodic scheduled and unscheduled audits” of those data security systems on behalf of NTIS.⁵

While we share the goal of maximizing data security protections for DMF data, we believe that attempting to impose specific additional requirements on financial services firms, to be monitored and enforced *via* audits, would risk undercutting the flexibility that is critical to combatting identity-related fraud and imposing additional operational burdens on financial services firms without any commensurate gain in data security. Financial services companies operate on the front lines of the battle against identity theft and are aligned with Congress in the goal of taking all reasonable measures to avoid fraudulent use of personal data. Given the increasing sophistication of the perpetrators of identity theft and other forms of financial fraud, financial services companies have developed highly sophisticated and continually evolving data protection régimes to safeguard the consumer data that they maintain in the ordinary course of business. These data-security measures have been highly successful at repelling identity theft and other forms of financial fraud, and we believe that maintaining flexibility on the part of financial services companies and anti-fraud vendors to react and innovate in response to evolving threats is critical.

In developing data-security régimes, financial services firms are subject to the requirements of the GLBA, which requires financial institutions to take steps to safeguard customers’ personal information – the same type of information that is available on the DMF. The GLBA’s data-security requirements were created specifically for financial institutions handling sensitive personal information and are therefore an appropriate

⁵ We note that Section 1110.201 of the Proposed Final Rule suggests that NTIS itself, rather than an Accredited Certification Body, may conduct such audits. *See also* Request for Comments at 17. This suggestion appears to be at odds with the statement that NTIS “carefully considered developing, within the agency, the capacity to evaluate the information systems, facilities and procedures of Persons to safeguard DMF information, as well as to conduct audits,” but concluded that “it is appropriate for Accredited Certification Bodies to conduct periodic scheduled and unscheduled audits of Certified Persons on behalf of NTIS.” *See* Request for Comments at 8-9. To the extent that financial services companies are subject to audit, we request clarification that any such audits will be conducted only by Accredited Certification Bodies given the level of technical expertise required to conduct such audits competently and efficiently.

yardstick for measuring the sufficiency of a firm's data-protection measures for purposes of DMF access. The GLBA's requirements are "similar" to those of section 6103(p)(4) of the Internal Revenue Code, and compliance with the GLBA with respect to Limited Access DMF data therefore satisfies the requirements for the proposed data-security certification. Under the circumstances, we believe that imposing additional requirements on financial services firms would not serve any meaningful purpose and may even be counterproductive. We therefore urge NTIS to create an exception to the proposed certification and audit requirements for financial services firms that commit to subject Limited Access DMF data to the same sophisticated and evolving data security measures that they apply to their customer data in accordance with the GBLA.

5. DATA-PROTECTION REGIMES APPLICABLE TO DMF DATA

NTIS proposes to amend section 1110.102(a)(2) and (3) to eliminate the requirement that persons seeking access to the Limited Access DMF certify that they will "satisfy the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986." We agree with this proposed amendment and urge that it be made final, for two reasons. *First*, the amendment would eliminate the conflict that existed in the Interim Final Rule between the requirement to abide by requirements "similar to" those set out in section 6103(p)(4) and the requirement to abide by the letter of Section 6103(p)(4).

Second, a requirement of strict compliance with section 6103(p)(4) would have the effect of preventing many financial services firms that rely on the DMF for important fraud-prevention functions from gaining access, notwithstanding that such firms necessarily have sophisticated data-protection measures in place. Section 6103(p)(4) was not designed to secure a massive electronic database such as the DMF, and it is not clear how certain aspects of section 6103(p)(4) – such as the requirement to establish a "secure area or place" where tax returns can be stored – would even translate to the DMF context. Compliance with the requirements of the GLBA is a more effective measure of data security than compliance with a statute designed for a different and arguably inapplicable context and should suffice for certification to avoid disrupting DMF access by firms that operate on the front lines of the battle against identity fraud. For these reasons, we support the proposed amendment.

6. FEES AND PENALTIES

The Proposed Final Rule adds a much-needed layer of due process to the penalty provisions set forth in the Interim Final Rule. While we commend NTIS for recognizing the need for due process in this regard, the proposed framework for appeal and review is inadequate insofar as it would give the Director of NTIS final say over the legitimacy of a penalty imposed by NTIS.

It is essential that companies facing potential liability by virtue of unscheduled audits and substantial financial penalties have well-developed procedural rights,

including the rights of appeal to an administrative law judge and ultimately to federal court. Otherwise, the penalty provisions risk creating a disincentive for financial services companies to use the DMF for fraud prevention, compliance activities, and other legitimate and important business purposes.

7. PAPERWORK REDUCTION ACT—PROPOSED COLLECTIONS OF INFORMATION

The Request for Comments states that NTIS is requesting approval of two forms for information collection: (i) the Limited Access DMF Systems Safeguards Attestation Form, and (ii) the Limited Access Death Master File Subscriber Certification Form. As of the date of this letter, these forms have not to our knowledge been made available to the public for comment. We reserve the right to submit comments on these forms if and when they become publicly available.

* * *

In light of the foregoing comments, FSR and BITS urge NTIS to adopt a Final Rule that:

- (i) clarifies that use of DMF data to facilitate payment to beneficiaries is a “legitimate business purpose” within the meaning of Section 203 and that third-party vendors that assist financial services firms with DMF search functions are deemed to have a legitimate fraud prevention interest within the meaning of Section 203;
- (ii) clarifies that disclosure to a beneficiary of the fact of death attributable to DMF data, without disclosing a decedent’s social security number, does not run afoul of the Proposed Final Rule;
- (iii) creates a carve-out from the audit and certification requirements for financial services firms that commit to subject DMF data to the same security measures applied to customer data under the GLBA; and
- (iv) enhances the “due process” protections for entities subject to audit or potential penalties, including an opportunity to be heard in an administrative proceeding and rights of appeal to federal court.

If it would be helpful to discuss our specific or general views on the Proposed Final Rule, please contact Richard Foster at Richard.Foster@FSRoundtable.org; Felicia Smith at Felicia.Smith@FSRoundtable.org; or Nancy Guglielmo at Nancy.Guglielmo@FSRoundtable.org. We appreciate your consideration and look forward to working with you on this important matter.

Sincerely Yours,



Richard Foster
Senior Vice President and Senior Counsel
for Regulatory and Legal Affairs
Financial Services Roundtable



Nancy Guglielmo
Vice President, BITS Fraud Reduction
Program
BITS

With a copy to:

The Honorable Penny Pritzker
Secretary
Department of Commerce

Henry Wixon, Esquire
Chief Counsel
National Institute of Standards and Technology