



March 30, 2015

Via [www.regulations.gov](http://www.regulations.gov)

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

RE: Certification Program for Access to the Death Master File (RIN 0692-AA21)

Dear Director Borzino:

This letter is submitted on behalf of Visa Inc. ("Visa") in response to the National Technical Information Service ("NTIS") Notice of Proposed Rulemaking on its Certification Program for access to the Death Master File ("Proposal") under Section 203 of the Bipartisan Budget Act of 2013 ("Act").

Through the certification program, NTIS seeks to ensure that access to certain information in the Death Master File ("DMF") is limited to persons that have a legitimate interest in the information, including for fraud prevention purposes, and meet certain additional requirements to safeguard that information to reduce opportunities for identity theft and other fraud. The Proposal would set forth requirements to become a certified person, establishes a process for third party attestation and auditing of an information safeguarding requirement for certification, provides for periodic audits, and sets out penalties for persons that improperly disclose or use DMF information.

Visa supports the efforts of NTIS, the Administration, and Congress to better secure the privacy of sensitive personally-identifiable information ("PII") through enhanced security procedures and protections. As it develops the final rule, we respectfully request that NTIS consider existing practices applicable to the safeguarding of sensitive Non-public Personal Information ("NPI") for financial institutions and their service providers and the audit controls and processes prevalent in the financial industry. We also urge NTIS to avoid unduly adding requirements that may lead to disruption in access and use of DMF information at the expense of protecting consumers from fraud.<sup>1</sup>

#### **I. The Use of DMF Access for Fraud-Prevention Purposes**

Financial services companies have significant interests in detecting and preventing identity theft and financial fraud and rely on tools that incorporate or access DMF data to meet these objectives and comply with their obligations under federal law (such as the Bank Secrecy Act and its implementing rules). Activities that require access to DMF data include vetting new customers seeking to open new accounts; assisting with

---

<sup>1</sup> In addition to the comments set forth in this letter, we support the comments submitted by the Financial Services Roundtable and BITS.

real time evaluations of credit underwriting; and detecting and identifying potential account takeover fraud or identity theft.

Many financial institutions rely on Visa's risk products as part of their fraud prevention and account management strategies. These products help reduce fraud within account origination to assist with real time evaluations of underwriting new applications while contributing to the mitigation of fraud associated with account takeover and identity theft. These products also improve account management to ensure that the most up to date information is received for ongoing evaluations of consumer credit risk and account and transaction fraud. For the vast majority of our products, Visa uses the DMF to provide financial institutions information for ongoing credit risk evaluations to help them reduce credit and fraud losses. Information provided through the DMF also helps our clients improve customer service by accurately identifying recently deceased customers and subsequently ceasing collection efforts, and assisting in the transition of those account relationships.

## **II. Certification Requirement Should Not Mandate a Separate Assessment or Review**

The Proposal would create a process by which NTIS could certify that a person seeking access to DMF information has a legitimate fraud prevention or other business purpose and sufficient information security systems, facilities, and procedures in place to protect the security of that information. Among other things, the Proposal would subject any entity seeking access to DMF information to submit a written attestation from an independent Accredited Certification Body (as defined in the Proposal) that the entity has information security systems, facilities, and procedures in place to protect the security of the DMF information. The attestation from the Accredited Certification Body must be based on a review or assessment conducted no more than three years prior to submission of a certification request or renewal request from the person seeking access to the DMF information; however, the review or assessment "need not have been conducted specifically or solely for the purposes of submission [of the certification request]."<sup>2</sup>

Visa agrees with NTIS that a separate review or assessment of an entity's information systems and processes for determining the adequacy of the entity's systems, facilities, and procedures is unnecessary to further Section 203's objectives. As NTIS has noted, "security and safeguarding of information and information systems is of great concern" beyond the use of DMF information, and that security and safeguarding assessments "are routinely carried out in the private sector."<sup>3</sup> For example, financial institutions commonly use independent CPA firms to perform annual assessments of their service providers' information security systems and controls under the internationally recognized SSAE 16 auditing standard. Under this standard, the CPA will conduct testing of control activities and render an opinion about whether in all material respects, the controls were suitably designed and operating effectively to provide reasonable

---

<sup>2</sup> See proposed Section 1110.502(b).

<sup>3</sup> See 79 FR at 78316.

assurance that the control objects were achieved during the test period. These assessments could be easily be modified or adjusted to include a review of a certified entity's systems, facilities and processes as they specifically apply to the retention of DMF information without imposing the additional costs or burdens of conducting an independent audit or assessment in order to satisfy NTIS' requirements.

### **III. DMF Safeguard Criteria Should be Consistent with Other Comparable Information Security Standards and Attestation Should Not Require "Absolute" Assurance of the Adequacy of a Person's Systems, Facilities, and Procedures**

Visa further requests that NTIS clarify that any written attestation required under NTIS' certification program should not require the Accredited Certification Body to provide "absolute" assurance of a certified person's information security systems, facilities, and procedures regarding the safeguarding of DMF information. Instead, it should be sufficient for the Accredited Certification Body to provide "reasonable" assurance consistent with industry practice regarding similar attestations under other information security related requirements, guidelines, or standards. Subjecting the DMF certification process to a higher standard than might apply in similar contexts could otherwise discourage auditing firms and others from agreeing to serve as an Accredited Attestation Body under this rule, and thereby present difficulties for persons seeking certification to receive DMF information.

### **IV. Rule Should Not Be Finalized Until NTIS Has Published a Revised Certification Form 161 and the Limited Access DMF Systems Safeguards Attestation Form For Comment**

Currently, a person seeking certification for eligibility to receive DMF information must submit a completed Certification Form NTIS FM161 (Limited Access Death Master File Subscriber Certification Form). Under the current form, a prospective subscriber to the Limited Access DMF must state either its fraud prevention interest or another business purpose for receiving the information and further certify that it will not disclose the DMF information to unauthorized persons or use such information for any purpose other than a legitimate fraud prevention interest or business purpose. NTIS has indicated it expects to update the Certification Form NTIS FM161 to collect additional information that will improve NTIS' ability to determine whether a person meets the requirements of Section 203 of the Act.<sup>4</sup> In addition, in the Paperwork Reduction Act section, NTIS states it is further requesting approval of an additional Limited Access DMF Systems Safeguards Attestation Form which Accredited Certification Bodies would be required to submit to attest that a person seeking certification to access Limited Access DMF information has the requisite systems, facilities, and procedures in place as required under the rule.

---

<sup>4</sup> See 79 FR at 78320.

To our knowledge, NTIS has yet to make these forms available to the public for comment. Visa respectfully requests that NTIS not move forward on finalizing this rulemaking until the forms have been made available to interested parties the opportunity to provide comment, as the forms could provide further opportunity for affected stakeholders to understand certain of NTIS' expectations regarding compliance with the rule. For example, proposed Section 1110.502(c) would require Accredited Certification Bodies to describe the nature of its review or assessment or audit where such review or assessment or audit was not conducted specifically or solely for the purpose of submission of a DMF access request. Providing the form for comment could provide an opportunity for potential certified persons and Certification Bodies to understand their obligations under the rule regarding this requirement.

#### **V. Existing Temporary Certification Forms Should Remain Valid Until NTIS Has Implemented Final Rules**

Finally, under its March 26, 2014 interim final rule (Interim Rule), NTIS established a provisional approach for implementing the Act's provisions pertaining to the certification program, including a mechanism for providing uninterrupted access to the DMF to users demonstrating a legitimate interest or purpose for the information upon the effective date of Section 203 of the Act. The Interim Rule provided a one-year certification term for parties that met NTIS' criteria under the Interim Rule. In the Proposal, NTIS has stated that persons that have previously obtained access to DMF information under the temporary certification program need not resubmit a request for certification pending NTIS' adoption of a revised final rule. In light of the initial one-year term for the temporary certification form, Visa respectfully requests that NTIS publicly extend the term until at least such time that a final rule becomes effective to avoid any disruption in receipt of DMF information by current certified entities that use the information for legitimate fraud prevention or other business purposes.

\* \* \*

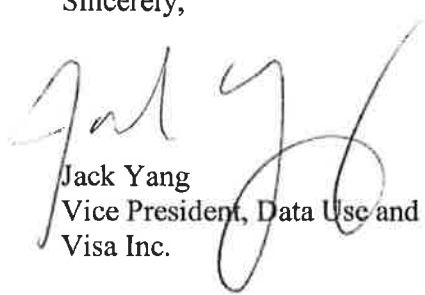
We appreciate the opportunity to share our perspective in this important matter. Visa and our partners in the financial industry rely on the DMF to identify fraud, stop identity theft, limit credit risks, and disrupt cybercrime. We urge NTIS in implementing a Certification Program that satisfies the purposes of Section 203 of the Act to avoid requirements that impose unnecessary or additional obstacles on entities seeking the information for legitimate fraud prevention or other business purposes. In particular, any undue disruptions or barriers to DMF access would expose the payments system to increased risk and consumer harm.

March 30, 2015

Page 5

If you have any questions concerning the issues raised in this letter, do not hesitate to contact me at 650-432-3817.

Sincerely,



Jack Yang  
Vice President, Data Use and Privacy  
Visa Inc.

