MEMORANDUM

TO: Grantees, National Foreclosure Mitigation Counseling Program

FROM: NeighborWorks America

DATE: May 25, 2010

RE: NFMC Program requirements on protection and disposal of clients' personal information

---

The NFMC Program would like to take this opportunity to remind all Grantees about the importance of responsible handling and disposal of clients' personal information. This element of NFMC Program compliance is informed by four sources:

- National Industry Standards for Homeownership Counseling;
- HUD's standards for approval of housing counseling;
- Applicable state laws that involve protecting personally identifiable information and preventing identity theft; and
- Applicable federal laws, including the Gramm-Leach-Bliley Act and accompanying regulations issued by the Federal Trade Commission.

1. National Industry Standards for Homeownership Counseling

All Grantees certify that they and their sub-Grantees will adhere to the National Industry Standards for Homeownership Counseling, a copy of which is included with NFMC Program funding announcements and grant agreements. In addition, Grantees are responsible for monitoring to ensure that all sub-Grantees and Branches adhere to the standards.

The National Industry Standards for Homeownership Counseling include recommended benchmarks for Recordkeeping. Two provisions specifically address the protection of clients' personal information: (1) Files should be maintained in secured file cabinets in order to protect client privacy. Scanned documents or electronic files should maintain the highest level of client security. (2) At the time of disposal, files should be shredded or electronic copies should be deleted.

2. Requirements for HUD Housing Counseling Approval

All Grantees must certify that they and their sub-Grantees meet or exceed HUD's requirements for housing counseling approval. In addition, Grantees are responsible for monitoring to ensure that all sub-Grantees and Branches adhere to the standards.

3. Applicable state and federal laws

NFMC Program Grantees are required to remain fully informed of all federal laws and regulations that apply to them, including the Gramm-Leach-Bliley Act and its accompanying regulations issued by the Federal Trade Commission ("FTC"). To protect consumer information and reduce the risk of identity theft, the Gramm-Leach-Bliley Act requires entities that possess consumer information for a business purpose to ensure the security and confidentiality of personally-identifiable information. Under this law, the FTC issued two rules that provide standards for safeguarding sensitive client information and disposing of client information:

The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The Disposal Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to:

- burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
- conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Due diligence could include:
    - reviewing an independent audit of a disposal company's operations and/or its compliance with the Rule;
    - obtaining information about the disposal company from several references;
    - requiring that the disposal company be certified by a recognized trade association;
    - reviewing and evaluating the disposal company's information security policies or procedures.

4. Applicable state and federal laws

Many states have passed additional laws to protect clients' personally identifiable information and prevent identify theft. Each Grantee is responsible for being informed about all state laws that may apply to its use and disposal of client information, and for satisfying the specific standard required in its own state. Grantees are also responsible for ensuring that their sub-Grantees and Branches are in compliance with the applicable laws of their respective states.