**Section 346.17 Database Procedures for Pilot Program**

a) Database for Program

Pursuant to Section 70(b) of the Residential Real Property Disclosure Act (Act), the Department shall establish a database in order to implement the predatory lending database pilot program. In any contract with the database vendor, the Department shall impose any relevant obligations and restrictions from the Act onto the database vendor.

b) Confidentiality

1) The database shall be designed so as to preserve the confidentiality of database information pursuant to the Act.

2) The Department shall further impose the following confidentiality restrictions on the database vendor:

A) The database vendor shall have in place written policies and procedures to safeguard confidentiality, and shall make those policies and procedures available to the Department. The Department shall not allow the pilot program to operate until it has reviewed those policies and procedures to its satisfaction.

B) The database vendor shall provide adequate supervision and training to its agents, employees and subcontractors to ensure confidentiality. The database vendor shall require its agents, employees, and subcontractors to sign an acceptable use policy as approved by the Department to ensure confidentiality and proper use of the system.

C) The database vendor shall specifically acknowledge the confidentiality restrictions imposed by the Act, and agree to abide by them.

c) Data Security and Transmission

1) All data transmitted to and from the database shall be converted into a secured format through encryption and 128 bit encryption shall be build into transmissions to and from the database system to prevent unauthorized viewing or tampering of encrypted information. The database shall also be required to encrypt social security numbers using the Advanced Encryption Standard (AES) issued by the National Institute of Standards and Technology (NIST), 100 Bureau Drive, Stop 1070, Gaithersburg MD 20899-1070, as Federal Information Processing Standards Publication (FIPS PUB) 197 (November 26, 2001, no subsequent amendments or editions are included). Data encryption will occur using a commonly used protocol for managing the security of message transmission on the Internet known as Secure Socket Layers (SSL). SSL shall be utilized for transmission of data through the Internet and the database.

2) The database shall incorporate a completely automated virus protection scheme. Procedures shall be put in place to ensure that all systems are updated on a regular basis and checked regularly for compliance with the current virus patch level. Procedures shall also be put in place to require that all information downloaded from external services or posted to the perimeter network are immediately scanned for viruses.

3) The database shall utilize for electronic transmission, rather than manual entry, of loan application information the rules and standards that the Federal National Mortgage Association (Fannie Mae) (established under authority of the Federal National Mortgage Association Charter Act (12 USC 1716, et seq.)) publishes for encoding mortgage loan application information into and electronic, computer-based format known as Fannie Mae Residential Loan Data Format 1003 (General Distribution Version, Version 3.2, March 17, 2005, not including later amendments or additions), Fannie Mae, 3900 Wisconsin Avenue, NW, Washington, DC 20016 (202) 752-7115. The Department may design other file formats for other uses of the system.

(Source: Added at 30 Ill. Reg. 14262, effective August 18, 2006)