Security/Confidentiality

Informatix, Inc. understands the importance of providing a secured physical and system environment for the data match project. Virtually all of our projects require a comprehensive security plan. Informatix has extensive experience with security through our many years of working with federal and state governments. Most importantly Informatix has provided services to the Child Support Program since 1990. Information maintained by child support staff and their vendors are subject to the same rigorous controls as banking records.

Informatix understands firsthand the types of sensitive information involved in managing child support operations and financial records. Our staff are knowledgeable in the requirements of Federal and State laws and regulations. Informatix maintains rigorous corporate standards regarding the security of information in our project offices. One of the services we provide to the child support community is operating payment processing centers. Currently, Informatix provides full payment processing services to eight states. These centers process payments and have access to state child support systems. Informatix has designed and implemented a comprehensive security plan to ensure that all data are used for only professional and authorized purposes. This security plan is also utilized for the FIDM project.

Informatix recognizes that Federal regulations impose stringent accountability and security requirements for the management of financial information. Informatix has adopted many layers of security to ensure guidelines are met to safeguard financial account records, and match result records. The first level of security is the physical processing center, which is accessible only by authorized personnel carrying correct access cards. The building itself is totally anonymous. There are no names or signs of any type on the exterior of the building or parking areas. The information regarding physical location is shared with the financial institutions through a cover letter in the outreach process. This instructs them where tapes are to be sent. The building contains general work areas and a secure computer room, where, again, access is limited to authorized technical and administrative personnel. Informatix provides additional site security through an extensive video camera surveillance system. Cameras are installed in all areas critical to the operation of the data match process. The next level of security is the computer systems security. Windows NT is used as the operating system of choice for the application. With this operating system, strict security is enforced. User ID and password access control the operation of all workstations within the processing center. The passwords will expire periodically and screen savers are password-protected. Database, application, and secure web access complete the protection of the data held within the processing center. When data are received at the secure website, users must pass through the normal access validation process before enabling the file transfer. The secure website uses the Windows NT security schema and forces users to enter valid IDs and passwords to access the system. Then, access is limited within the website, depending on a specific user's access level. Physical files received at the center are logged in by authorized personnel. These staff members do not have access to the internet nor do they have CD writers or disc drives on their workstations, thus preventing

them from duplicating files. Once logged in these files are passed to authorized personnel with access to the upload processes for updating the database servers with the IV-D data and financial account details. The database servers are placed on secure directories, accessible only by the application programs used to perform the match and authorized personnel who have access to the match routines. The database of choice is Oracle, which has extensive security schemas over and above the Windows NT model. This will prevent unauthorized access to the data records. This highlights the security measures that have been adopted at the processing center to ensure the financial institutions that Informatix takes data safeguarding very seriously.

The data received by Informatix for the FIDM project is only used for the match and results processing. This data is highly secured and used for no other purpose than to build and maintain a database of IV-D case arrearage records (obligor database), receive and process financial account records against the obligor database, format the result records, and return the data to the requesting donor states. Data is archived to physical media at agreed-upon intervals and deleted from the database, and the archives will be returned to the donor states. Data will be disclosed only to personnel authorized to handle the data files and process the match and results records. Physical files received from financial institutions will be returned upon conclusion of the processing or used for the next quarter obligor extract and effectively overwritten by the new file. No data records are kept that are not required by the processing center after the end of the quarter and after the states have accepted the results. Financial institution records will not be written to a database; they will be used as the basis for the match and stored only if a positive match is made that requires the account information to be returned to the state.

Additional safeguarding of data:

Policies and procedures – Informatix maintains on an ongoing basis policies and procedures for managing the complete operation of the processing center. This includes all necessary security measures; access rights; and proper handling of the data files, from receipt to return.

Screening, training, bonding, and non-disclosure oaths of personnel - As part of our hiring process, Informatix conducts complete background checks on all applicants. Additionally, all staff assigned to the data match project are bonded. Staff in the processing center are also required to store all personal belongings (coats, handbags, etc) in lockers located away from the processing environment.

Detection of unauthorized/illegal activities - In order to further safeguard the data from unauthorized/illegal access, Informatix has added two extra levels of control to the information bank:

- An encryption algorithm will scramble important data fields, such as SSNs and financial account numbers. The application will unscramble these fields when processed for the results file, to be returned to the Participating States. The NT security schema has also been created to secure the directories containing these

data fields so that they will not be accessible by unauthorized personnel within the operational center. Floppy disks have not been installed on operational workstations within the processing center, making it very difficult to copy files to a removable medium. Only the network servers within the secured computer room are installed with the necessary floppy drives. Additionally only the workstations in the secured server room have access to the internet.

- The application security subsystem, as well as the NT security schema have alerts and audit trail logging enabled. This will notify administrative personnel of attempted violations. The security subsystem controls access to all parts of the system; when certain data are requested, it is set up to log the event, User ID, date and time key data requests, etc. This enables close scrutiny of operational data access, which is reviewed by the management personnel as required.

- Retention and disposition of data- When receiving information from financial institutions utilizing Method 1. Informatix will load the tape and run for possible matches, all names which do not result in an immediate match will be automatically dropped from the file and will not be stored on the server.

Informatix wishes to ensure all financial institutions of our commitment to proper handling of sensitive financial information. Should you have further questions please feel free to contact me at us at (877) 965-3436.