

**Minutes of
Identity Theft Committee
December 8, 2006**

The Identity Theft Committee met at 99 East River Drive, East Hartford, in Room 707 on Friday, December 8, 2006 from 1:05 PM to 3:15 PM.

Those in attendance: Judge Berger, Judge Blawie, Mr. Callahan, Atty. D'Alesio, Atty. Fisher, Professor Marsh, Det. Peterson, Judge Pellegrino, Judge Pittman, Atty. Roberts, Atty. Shay, Atty. Stillman, Atty. Ury, and Atty. Yen.

Judge Pellegrino called the meeting to order at 1:05 PM. The first agenda item was the review of the minutes of the last meeting. Upon motion and second, the minutes were unanimously approved as distributed.

The next agenda item was a discussion of Aetna's experience with identity theft. Rob Stillman provided an overview of Aetna's approach and some of the information they learned in their tackling the problems of protecting information. He indicated that Aetna had realized that identity theft was only a piece of the larger issue of information privacy. Although the type of information and scope of access may differ, certain concerns that Aetna faced, including handling a large volume of data, needing strong firewalls, analyzing the means by which information leaves the office (laptops, personal storage devices, outside vendors, email data transmission), and the need to educate employees on the importance of protecting information are equally applicable to the Judicial Branch. In sum, Aetna's experience emphasizes that information privacy as a whole and protecting against identity theft specifically will require a combination of technological, personnel, and cultural adjustments.

Attorney D'Alesio then presented a proposed process for approaching the issue of identity theft through answering six questions that would include the identification of the types of information that could lead to identity theft, where the information is found, determining why we collect/receive the information, whether we should continue to collect it, how we protect the information we continue to collect/receive, and how we prevent the submission of information we determine that we do not need. The consensus was that the questions would serve as a basic roadmap for the committee, and other issues could be raised within the general framework.

The next item on the agenda was a discussion of the types of information that might need to be protected. Mr. Callahan presented information on regulations of financial institutions which result in the financial industry setting in place policy standard and procedures for identifying information that must be protected and providing protection for that information. He indicated that it is not possible to eliminate all risk from our environment, but you must "scope" what you are dealing with to arrive at the information you really want to protect and then put your resources toward protecting that information. Generally, pursuant to the regulations (both state and federal under the Gramm-Leach-Bliley Act) account numbers associated with a customer and social security numbers are personally identifiable information that would be protected. There was also a brief review of the interim report of the President's Task Force on Identity Theft, which basically was concerned with protecting social security numbers. The committee then identified information that could lead to identity theft: social security numbers, account numbers, (credit and bank account), date of birth, mother's maiden name, tax payer

Identity Theft Committee

12-8-06

Page 2 of 2

identification number, employer identification number, alien registration number, driver's license number, health insurance identification number, passport number, biometric data, address, name, place of birth, name of employer, place of employment, phone number, email address, names of minor children, name of spouse, PIN numbers, bank name, location and list of assets (stock and bond information), tax returns, marital status, and medical information. The list may be expanded as the committee continues its discussions.

The next item on the agenda was a review of other states' policies and rules on sensitive/confidential information. Handouts were provided to the committee, containing the information on the survey of the states. There was also a brief discussion of the status of the review of court forms, specifically forms available on the website which request date of birth, social security number, or account numbers. Judge Berger pointed out that most forms are not rule-driven so that changes in the forms could be made quite easily. For the next meeting, staff will ascertain which forms are most frequently found in the court files.

Attorney D'Alesio then pointed out Sec. 4.20 and Sec. 4.60 of the Proposed Policy on Access to Court Records, indicating that this committee will be concerning itself with those two sections specifically in connection with its work on identity theft. Also, in connection with the Public Access Task Force, he said that the Branch will post criminal docket information online, and one of the questions that the Task Force had was about the inclusion of the birth date online. The consensus of this committee is that only the year of birth should be posted online.

Next, the committee returned to a discussion of the questions, specifically looking at why the branch collects this information. Judge Pittman raised the issue of exhibits and other documents that the courts receive on a temporary basis versus those that are received on a permanent basis. As files become electronic, the branch may want to eliminate some of what it collects. A discussion ensued as to why certain information is solicited by or submitted to the courts, i.e., case law, custom, culture, court order, practice book rule, and federal or state statute. Also, various additional reasons were raised for the court's collection of this information, i.e., academicians' study, certainty of identification, statistical purposes, etc. There was also discussion of how to handle confidential information that is submitted: refusing to accept documents without the information's having been redacted, changing the culture to accept filings without this information, or holding a hearing under P.B. Sec. 11-20A to redact information. Suggestions were made as to how to ensure the compliance of the Bar in any changes to be made in the filing of confidential information and how to effect changes from the "top down" so that judges are more sensitive to this information.

It was pointed out that the Branch collects social security information from outside vendors among others. Judge Blawie said that the protection of information comes down to risk management, and the Branch must take care of its files.

The next step is to identify and to locate all the rules and statutes that require any of the information that the committee identified as potentially leading to identity theft. Staff will assemble this information for the next meeting which will be held in late January. Information on that meeting will be emailed to members of the committee.

The meeting adjourned at 3:15 PM.