

**Testimony on Interagency Regulatory Information Sharing
before the
Committee on Financial Services
Subcommittee on Oversight and Investigations
Subcommittee on Financial Institutions and Consumer Credit
United States House of Representatives
March 6, 2001**

**Scott Albinson, Managing Director, Supervision
Office of Thrift Supervision**

I. INTRODUCTION

Good afternoon, Chairman Oxley, Chairwoman Kelly, Chairman Bachus, Ranking Member LaFalce and Members of the Subcommittees. Thank you for the opportunity to discuss the interagency regulatory information sharing systems we have in place at the Office of Thrift Supervision (OTS). We support the efforts of this Committee to improve information sharing among the financial regulators. Safeguarding thrifts from fraudulent activities and from individuals and entities responsible for financial fraud is of paramount concern to OTS. We have spent considerable time and effort, particularly over the last several years with the increase in insurance and securities affiliations in the thrift industry, to improve our ability to access the most recent and useful information on fraud in all sectors of the financial services industry.

We also appreciate the attention that has been directed at-and urge the Committee to continue to be mindful of-the need to protect sensitive database information in attempting to craft an interagency database network. Finally, we support efforts to include confidentiality and liability protections for all shared information so that financial regulators do not compromise existing legal privileges when sharing database information with other financial regulators and law enforcement organizations.

II. RECENT THRIFT APPLICANTS AND OTS REGULATORY RELATIONSHIPS

Since 1997, 43 insurance groups and 15 securities firms have acquired or affiliated with an OTS-regulated savings association. For all applications, OTS is required by statute to review and evaluate the financial and managerial resources of the applicant. This process is intended to identify, to the extent practicable, the extent to which an acquisition or affiliation poses risks to the safety and soundness of the thrift institution. As you may surmise, this can be a daunting task, particularly if the applicant has financial affiliates throughout the country and in various businesses of the financial services sector.

It is not uncommon for us to consider applications in which an applicant or its affiliates has a significant presence in almost all of the 50 states, as well as U.S. territorial and foreign business operations. Assuming for example that the applicant is engaged in the business of insurance, we may have to contact the state insurance commissioner in each state in which the applicant or its affiliates conduct business. Where an applicant has both securities and insurance operations, the relevant information trail may lead to the Securities and Exchange Commission (SEC), the National Association of Securities Dealers (NASD), and the office of many state securities commissioners.

Pursuant to our statutory standards of review, OTS has been sharing information with various state and federal regulators for some years. Our information sharing arrangements are both formal and informal. We work closely with other federal banking agencies and state bank regulators, both through the Federal Financial Institutions Examination Council (FFIEC) and individually, where appropriate, to identify emerging issues in the financial institutions industry and to coordinate supervisory activities. In some

cases, we have written agreements to share information with state banking agencies, and in other instances our relationship is more informal. We have a longstanding working relationship with the SEC and, in 1995, we developed and signed a formal written information sharing agreement with NASD (see attached).

The influx of insurance company applicants for thrift charters during the late 1990s prompted us several years ago to develop a close working relationship with the National Association of Insurance Commissioners (NAIC). This led to development of a model agreement that is the basis for written information sharing agreements between OTS and 41 states, including the District of Columbia (see model agreement and list of states, attached). These joint agreements extend significantly beyond the sharing of consumer complaint data and include the sharing of financial and enforcement information, including prior notification regarding enforcement action taken against a commonly regulated entity. We hope, ultimately, to have agreements in place with every state insurance commissioner, as well as with the insurance commissioner of every U.S. territory. Three states-Rhode Island, Ohio and Oregon-have told us that they need to change their states' laws to allow for such information sharing, which we understand they plan to do this year.

Our ability to share confidential information with the NAIC itself is limited, since it is not a governmental entity. Because the NAIC plays a significant role in the work that is done by and for the state insurance regulators, it would be beneficial for OTS to be able to exchange information with the NAIC.

III. OTS INFORMATION DATABASES

OTS maintains or contributes to three separate databases that include information on individuals and entities that have participated in illegal conduct. Each database serves a different function.

The first database lists public enforcement actions taken by OTS since 1989. The list, which is updated monthly, gives the name of the individual or entity subject to the enforcement action, the name of the institution, and the type of order issued. We have posted on our website OTS orders removing or prohibiting individuals from insured depository institutions. The list is searchable by the name of the individual, company or savings association. We will be expanding the list to include other types of OTS orders, such as cease and desist orders and civil money penalty assessments, and to post actual copies of the orders to the website.

The second database is our Confidential Individual Information System (CIIS). These records contain information concerning individuals who have filed notices of intent to acquire control of savings associations; individuals who have applied to become senior officers or directors of savings associations (where such review is required); individuals who have a history of professional ethics, licensing, or similar disciplinary problems, or have been the subject of an agency enforcement action; and individuals involved in a significant business transaction with an institution. These records identify the individual involved and his or her relationship to the savings association, service corporation or holding company, and describe the event causing the entry of information into the CIIS database. These records are confidential under the Privacy Act of 1974. Consistent with the limitations under the Privacy Act, OTS shares this information, upon request, with other governmental and self-regulatory organizations, such as the SEC, Commodities Futures Trading Corporation (CFTC), and NASD Regulation (NASDR).

The third database we utilize is the Suspicious Activity Reports (SAR) database, which the OTS contributes to, along with the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), National Credit Union Administration (NCUA) and the Financial Crimes Enforcement Network (FinCEN). This system contains reports that

banks, thrifts and credit unions are required by federal statute to file whenever they have information concerning suspected violations of certain criminal statutes, such as bank fraud, theft and money laundering. An example would be when a depository institution notes that an individual has made several cash withdrawals from an account, all of which are close to but just below the level at which the bank must file a Currency Transaction Report (CTR).

Because the SAR database contains highly confidential information of known or suspected criminal activities, on-line access to the database is restricted to the banking regulatory agencies, certain other federal agencies, and to law enforcement agencies, such as the Federal Bureau of Investigation (FBI) and the Secret Service. Unauthorized access to this information could substantially jeopardize law enforcement investigations. It could also cause unnecessary harm to individuals whose names are included in SARs as possibly involved in suspicious activities, but where the matter has not been investigated and which may prove to be not true. Banks and thrifts are prohibited from disclosing a SAR or its contents, and bank regulatory agencies do not share SAR information with non-SAR users.

In addition to coordinating on the SAR database, the banking agencies participate with the SEC, Internal Revenue Service (IRS), U.S. Customs Service, and law enforcement agencies, including the FBI and Secret Service, in the national Bank Fraud Working Group. This forum enables these agencies to share information on and cooperate in identifying individuals engaged in fraud and trends involving fraudulent activities. Important interagency information sharing activity also occurs outside of Washington. Many U.S. Attorney offices convene several meetings each year to discuss bank and financial fraud issues and activities. Participating agencies usually include the federal banking agencies and state insurance and bank regulators. NCUA representatives may also attend. These meetings provide an opportunity for the U.S. Attorney offices to discuss ongoing bank fraud cases, to the extent the information is disclosable, and to alert regulators about recent patterns of criminal activity. The regulators also exchange information about possible criminal activities within their jurisdiction, including information brought to their attention by SAR filings.

IV. POSSIBLE APPROACHES TO INTERAGENCY INFORMATION SHARING

The possible approaches to interagency information sharing vary depending on the type and sensitivity of the information to be shared, the availability and quality of the information on existing agency databases, and the ability to control access to and use of information. Also important are confidentiality and liability protections for shared information, and avoiding over reliance on shared information by users.

Among the range of available options, a practical first step is linking or aggregating the existing public databases of financial regulators. This, of course, assumes that all relevant financial regulators maintain similar types of information and make it publicly available. This option could be accomplished by creating a software link that permits each agency to operate their individual databases separately, but that makes the databases accessible simultaneously via a common search engine or able to be viewed from the same site. This is largely a software solution that improves efficiency by minimizing the number of times a user must search multiple places for the same information. Since the information is public, issues regarding liability and confidentiality should not be problematic. While access to the linked data could be limited to the financial regulators, it would not have to be, and information that is distributed beyond the linked network should not raise concerns since the information is already public.

While a software link is likely the most efficient approach because it is easiest to implement and poses the fewest potential problems, a centralized coordinator of public database information could also be established. This option is worth considering if there is an overall plan ultimately to expand or modify the system to include non public information.

Expanding the system to include nonpublic information, of course, raises a series of far more difficult issues, and would probably require a more centralized approach. Either a new or existing governmental entity could be charged to coordinate a type of centralized clearinghouse for the collection and dissemination of regulatory database information, and be made responsible for limiting access to the information, defining the parameters for the types and quality of information to be fed into the system, and providing liability and confidentiality protections. This raises obvious, but no less compelling logistical issues, such as how to coordinate the information, who should do so, how to eliminate obstacles about the governmental status of entities that participate in the system (i.e., in order to avoid issues raised about breaches of confidentiality and liability protections), and how to keep the system current. More important are issues involving protecting the integrity of system information-ensuring the information is complete and correct-and ensuring that otherwise non-public information does not fall into the wrong hands.

Variations of this approach include a system in which different levels of "security clearance" are provided to various users for accessing different strata of information. For example, all could access publicly available information, but more sensitive information on current or ongoing agency actions would be made available on a more select basis, with criminal investigatory information carrying the most protections. Also worth considering is whether more than one entity could serve as the aggregator of regulatory information. For example, three separate entities could be charged with collecting information-one each for securities, insurance, and banking information-and could then coordinate in establishing, feeding, and maintaining a centralized system.

A point worth emphasizing that is relevant to all of the variations and permutations described above is that for any type of database sharing system to be useful, particularly with respect to tracking the comings and goings of questionable individuals in the various financial services industries, the quality and integrity of the information fed into the system must be reliable.

Currently, the federal banking agencies are not routinely provided information regarding the addition of new directors and senior officers to a depository institution. The Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) required a 30-day prior notice to the appropriate banking agency upon the addition of a director or senior officer at a recently chartered depository institution, an institution or holding company that underwent a change in control within the preceding two years, and an institution or holding company not in compliance with minimum capital requirements or otherwise troubled. As part of the regulatory burden reduction provisions of the Economic Growth and Regulatory Paperwork Reduction Act of 1996, the prior notice requirement was narrowed to cover only troubled institutions and holding companies, capital-impaired institutions, and certain institutions operating under a capital restoration plan.

Although we do not advocate restoring FIRREA's original requirements, it would be beneficial to consider requiring a streamlined, after the fact notice to the appropriate banking agency of all new directors and senior officers of depository institutions. Consideration should also be given to including an appropriate mechanism for the prompt removal of a new director or senior officer where the banking agency determines that the individual has a past history of serious disciplinary problems in the financial industry. This would ensure that, as new directors and senior officers begin to serve at an institution, the agency has the information to conduct a background check and the ability to remove the individual where there is such past history. In addition, the agency would then be able to make the information immediately available to all other financial regulators. Currently, this information is not likely to be obtained until the next regularly scheduled examination of the institution, which could be up to 18 months from the time of the addition.

Another tool worth considering in addressing the problem of identifying and weeding out perpetrators of

financial fraud is a corporate governance self-help provision that an institution could include in its bylaws. OTS will soon adopt a regulation that permits, but does not require, federal savings associations to adopt a bylaw amendment precluding persons who are under indictment for, or have been convicted of certain crimes, or are subject to a cease and desist order for fiduciary violations entered by any of the federal banking agencies, from being a member of the institution's board of directors. This affords an institution a certain degree of self defense from perpetrators of financial fraud.

V. CONCLUSION

Fraud in the financial services industry is not new. What is new are the technological developments and innovations that have dramatically raised the stakes in identifying and weeding out fraudulent activities and bad actors. Each new advance that facilitates the potential for fraud compromises the integrity of our financial system and exposes Americans to greater risks in their financial dealings. The tools that new technologies provide can also be harnessed to help us fight fraud. And it is incumbent upon us to utilize these resources to preserve and maintain control of our financial systems.

All financial regulators spend considerable resources in tracking down fraudulent activities and the perpetrators of financial fraud. To the extent we can combine and leverage our collective experiences and information, our efforts will be that much more effective. As I noted at the outset, there is a delicate balance between effective information sharing and protecting sensitive database information. No one can refute that access to more, high quality information will improve our ability to fight fraud; but what do we give up to get there? Striking the proper balance is the key.

Thank you. I will be pleased to take any questions.