

GAO

Testimony

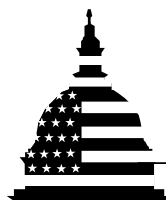
Before the Subcommittee on Oversight and Investigations
and the Subcommittee on Financial Institutions and
Consumer Credit, Committee on Financial Services
House of Representatives

For Release on Delivery
Expected at
2:00 p.m. EDT
on Tuesday
March 6, 2001

FINANCIAL SERVICES REGULATORS

Better Information Sharing Could Reduce Fraud

Statement of Richard J. Hillman
Director, Financial Markets and
Community Investment



G A O

Accountability * Integrity * Reliability

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

GAO has long held the view that financial regulators can benefit from greater information sharing. We have previously reported on the potential for rogues, as highlighted by Martin Frankel's alleged activities, to migrate between different financial services industries. In addition, a more integrated financial services industry as envisioned by the passage of the Gramm-Leach-Bliley Act highlights the need for strong information-sharing capabilities among financial services regulators.

This statement focuses on: (1) systems used by financial regulators for tracking regulatory history data, (2) regulatory history data needed to help prevent rogue migration and limit fraud, (3) criminal history data needs among financial regulators, and (4) challenges and considerations for implementing an information-sharing system among financial regulators.

Systems used by financial regulators for tracking regulatory history data are operated and maintained separately in the insurance, securities, futures, and banking industries. Each industry operates systems and databases that provide background information on individuals and entities, consumer complaints, and disciplinary records within that industry. Within the insurance, securities, and futures industries, this information is largely centralized. In contrast, such systems and databases are decentralized among regulators within the banking industry.

Regulatory history data needed to help prevent rogue migration and limit fraud include information on completed disciplinary or enforcement actions, ongoing investigations, consumer complaints, and reports of suspicious activity. Most regulators are in agreement about sharing regulatory information related to an individual's registration or licensing status and closed, or completed, adjudicated regulatory actions. Concerns remain over the sharing of other nonadjudicated regulatory information.

Criminal history data needs of regulators are focused on access to nationwide criminal history data. Currently, insurance regulators are not on equal par with their counterparts in the banking, securities, and futures industries, since many cannot obtain such data.

Challenges and considerations for implementing an information-sharing system among financial regulators are focused more on legal rather than technical issues. We found substantial agreement among the regulators about the benefits of sharing regulatory and criminal data in a more automated fashion. To accomplish this, it is clear that Congress will need to address confidentiality, liability, privacy, and other concerns.

With the Subcommittees' support, we believe that fraud prevention efforts among financial services regulators can be enhanced.

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

Subcommittee Chairs and Members of the Subcommittees:

We are pleased to be here today to discuss our observations on the sharing of regulatory and criminal history data among financial services regulators. GAO has long held the view that financial regulators can benefit from greater information sharing. Let me point to a couple of examples. In 1994, we recognized the potential for unscrupulous, or rogue, brokers to migrate freely from securities to other financial services industries and related industries, and we recommended expanded information sharing among financial regulators.¹ More recently, we reported on an insurance investment scam allegedly perpetrated by Martin Frankel, who had been barred for life from the securities industry. Mr. Frankel moved to the insurance industry, where he allegedly stole about \$200 million over an 8-year period.² Our report noted that many of those losses could have been avoided had more information been shared among regulators. Moreover, with the passage of the Gramm-Leach-Bliley (GLB) Act, the opportunity for banking, insurance, and securities products to be sold under the same corporate umbrella highlights the need for strong information-sharing capabilities among the financial services regulators.

In my statement today, I will first provide an overview of the systems currently used by insurance, securities, futures, and banking regulators for tracking disciplinary and other regulatory information. Second, I will discuss the data needs of regulators that would allow them to better prevent the migration of rogues from one industry to another and limit

¹ Securities Markers: Actions Needed to Better Protect Investors Against Unscrupulous Brokers (GAO/GGD-94-208, Sept. 14, 1994).

² Insurance Regulation: Scandal Highlights Need for Strengthened Regulatory Oversight (GAO/GGD-00-198, Sept. 19, 2000).

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

fraud. Next, I will discuss regulators' needs for criminal history information and barriers faced by some financial regulators. Finally, I will discuss some of the regulators' concerns about problems that could arise from sharing regulatory information through a more automated system.

In addition to reviewing our past work on these issues, we have had discussions with and reviewed available documentation from representatives of the National Association of Insurance Commissioners (NAIC), the Securities and Exchange Commission (SEC), the National Association of Securities Dealers Regulation, Inc. (NASDR), the North American Securities Administrators Association (NASAA), the Commodity Futures Trading Commission (CFTC), the National Futures Association (NFA), the Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), the Federal Deposit Insurance Corporation (FDIC), the Conference of State Bank Supervisors (CSBS), the Federal Financial Institutions Examination Council (FFIEC), the Federal Bureau of Investigation (FBI), and the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). Each regulator maintains systems for tracking information being discussed here today.

In our discussions we found substantial agreement among the regulators about the potential benefits of improved information sharing, particularly related to licensing or registration data and adjudicated regulatory actions. Most also concurred that it would be useful to share regulatory and criminal history information in a more automated fashion. However, each also raised concerns about various issues including confidentiality, liability, privacy, and the potential negative effects of premature disclosure of unadjudicated actions. As a result, developing and implementing a useful information sharing approach will require the Congress to address

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

many challenges, including concerns and potential inertia from some regulators about certain types of information sharing.

Overview of Financial Regulatory Information Systems

We found that most financial services regulators kept background and disciplinary-related data on individuals and entities in their particular financial industry.³ Within the insurance, securities, and futures industries, when regulators have authority to license or register individuals to sell financial products, this information is largely centralized. Each of these industries operates systems and databases that provide background information on individuals and entities, consumer complaints, and disciplinary records within that industry. In the banking industry, where regulators do not license or register individuals, we found that regulators also entered and maintained background, regulatory history, lending practice, and complaint data on entities and some individuals. Within in the banking industry, such systems and databases are decentralized among the separate regulators. Therefore, unlike the “one-stop shopping” search capabilities available in other financial industries, a search on an individual’s regulatory history in the banking industry could necessitate separate inquiries of the five regulators’ systems.⁴

Insurance

In the insurance industry, NAIC serves as the data administrator for the regulatory information systems and databases that serve each of the state insurance departments. According to NAIC, regulatory information on

³ Regulatory background information, among other things, would include the licensing or registration status and employment history of an individual.

⁴ Federal banking regulators include the FRB, OCC, OTS, FDIC, and the National Credit Union Administration.

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

over 5,200 insurance companies and nearly 3 million agents throughout the country is available to all state insurance regulators. Some of the key databases administered by NAIC include

- the Producer Database (PDB), a central repository of producer licensing information on agents and brokers that is updated daily with information provided by state insurance departments;
- the Regulatory Information Retrieval System (RIRS), a database of official regulatory actions taken against insurance agents and companies;
- the Directors and Officers (D&O) Database, a collection of company officer data derived from insurers' annual statements that, among other things, allows regulators to track the movement of these individuals from one entity to another (initiated in 1999);
- the Complaints Database System (CDS), a database of closed customer complaints made against individuals or firms; and
- the Special Activities Database (SAD), a database intended to facilitate the exchange of often unsubstantiated information that could be of regulatory interest to insurance regulators, including, in some cases, ongoing investigations.

To simplify queries for information, NAIC has also developed an Internet search application for insurance regulators called I-SITE that can query all of the above databases at the same time and return a combined response. Information from PDB and RIRS are accessible by state insurance regulators and commercial customers; the D&O, CDS, and SAD databases are only accessible to state insurance regulators. Although these databases are maintained by NAIC, much of the information must be supplied by regulators in the individual states, and the extent of such participation varies across the states.

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

Securities

Within the securities industry, NASDR administers the Central Registration Depository (CRD) system, the primary information system used by securities regulators to search for background information on individuals and firms. CRD can be used to obtain background information on an individual's registration status and employment history.⁵ CRD also contains "disclosure" data that includes an individual's criminal history, disciplinary actions taken on the individual by a federal or state securities regulatory authority, and disciplinary actions taken by a self-regulatory organization (SRO). Disclosure items on CRD also include civil judicial actions and open and closed customer complaints tied to the activities of individuals or firms.⁶ According to NASDR, approximately 10 percent of CRD records contain disclosure information.

The CRD system is accessible by federal and state securities regulators and SROs as well as by securities firms and broker-dealers; however, the amount of information disclosed varies. NASDR has allowed some other regulatory and law enforcement agencies access to CRD as well. Additionally, NASDR, through its statutory public disclosure program, releases certain disciplinary and other background information to the public on request. To facilitate public access to CRD, NASDR developed Web CRD, offering limited access to CRD through the Internet, although responses are not viewable on NASDR's Internet Web site and must be mailed or e-mailed to the requestor. SEC officials noted that much of the information on CRD is self-reported by broker-dealer firms and unverified.

⁵ In addition to registered individuals, CRD also contains records of unlicensed individuals who have been involved in the securities industry.

⁶ CRD contains consumer complaints involving sales practice violations that have been settled for more than \$10,000 or sales practice or fraudulent practices that contain a claim of \$5,000 or more in damages within the past 24 months. Complaints older than 24 months are archived and are subject to more limited disclosure.

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

Futures

Regulators of futures markets have also developed systems and databases to collect background data on individuals and firms associated with the futures markets. NFA maintains background information on individuals and firms in the futures markets on the Background Affiliation Status Information Center (BASIC) system. The BASIC system includes disciplinary actions taken against firms and individuals by CFTC, NFA, or an SRO. It also includes pending disciplinary actions by CFTC and NFA, but only final actions by SROs. Closed customer complaints can also be found on BASIC. According to NFA officials, nearly 6 percent of individuals in the BASIC system have records of regulatory actions associated with them.

Although the BASIC system is accessible to the public, a number of other databases maintained by NFA are not. The Membership Registration Receiver System (MRRS) is an automated registration processing system that collects registration data on firms, principals, associated persons, and floor brokers. The Financial Analysis Compliance Tracking System (FACTS) is NFA's internal record of all financial and compliance data on registered member firms and individuals. This system also includes information on open investigations, audits, criminal record checks, and consumer complaints. The Fitness Image System is another database that includes scanned-in documents associated with registered firms and individuals.

Banking

Within the banking industry, different bank regulators operate and maintain their own separate systems. Several banking regulatory officials pointed out to us that in contrast to the practice in other financial services industries, individuals who work in the banking industry and deal with the public are not registered or licensed. Consequently, since information

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

systems and databases used in the banking industry do not have to support such functions, they are not, in some respects, comparable to the systems used by other financial regulators. Although each bank regulator maintains its own databases of completed enforcement actions taken against individuals or institutions, regulators told us that, in general, communication among the banking agencies is good.

Additionally, working together with law enforcement agencies, bank regulatory agencies developed a single form, the Suspicious Activity Report (SAR), for the reporting of known or suspected criminal law violations and transactions that an institution suspects involve money laundering or violate the Bank Secrecy Act. Financial institutions enter these SARs into Treasury's FinCEN system. FinCEN provides support to over 150 federal, state and local law enforcement agencies, as well as to bank regulators and many international financial crimes investigators. FinCEN is a key element in efforts to prosecute money laundering and to "follow the money" to identify and apprehend criminals in this country and around the world.

Most enforcement actions taken by bank regulators have been public since 1989. Banking regulators are generally required to publish these actions and, additionally, have made such information available through their web sites. Recently, in cooperation with the FFIEC, bank regulators have created a set of links between their individual Web sites to facilitate Internet access to disciplinary or enforcement actions taken against individuals and institutions. Although the level of disclosure varies somewhat with each regulator, all disclose information on closed enforcement actions, such as removal and prohibition actions taken against officers and directors of an institution. Other actions posted by regulators include cease and desist orders and civil monetary penalties.

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

However, it is not always possible to determine from the posted data what specific behaviors or activities resulted in an enforcement action.

Banking officials also told us that each regulator maintains information on open investigations and consumer complaints. Upon request, banking regulators may share information on open investigations with other regulators. They may also contact other regulators including SEC or NAIC to coordinate actions, if appropriate. Most banking regulators are working through NAIC to establish agreements with state insurance regulators. Banking regulators stressed that consumer complaints that they receive usually do not involve bank officials, officers, or illegal acts. Complaints typically involve such areas as fee and service charges, error resolution procedures, interest payment calculations, or issues associated with bank closings or mergers. Regulators monitor trends in consumer complaints and follow up on them during bank examinations.

Improved Regulatory Data Sharing Could Help Prevent the Migration of Rogues and Limit Fraud

In discussions with financial regulators and Committee staff, four types of data, aside from those related to licensing and employment history, used by regulators could be useful in detecting fraud and limiting its spread from one financial industry to another. These data types are 1) completed disciplinary or enforcement actions, 2) ongoing regulatory investigations, 3) consumer complaints, and 4) reports of suspicious or unverified activity that merit regulatory attention, but may not yet rise to the level of a formal investigation. Some of these data types are not sufficient by themselves to support a regulatory action such as a disqualification for registration or a license. However, if regulators had the information available, it could prompt them to ask more probing questions or conduct further checks to ensure the fitness of industry applicants. In the Frankel case, although Frankel himself allegedly used aliases and fronts to perpetrate the fraud, one of the individuals who appeared to have provided funds to purchase

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

the first insurance company, subsequently looted of its assets, had a disclosure item involving complaints and settlements in the securities industry. If regulators had interviewed that individual to discuss past regulatory incidents and probed further, they may have found out that the individual had not actually provided the funds to acquire the insurance company and the scam may have been stopped before the assets were stolen.

Nearly all financial regulators maintain records and databases that include each of the above types of information—some as public information and some for use by only regulators or law enforcement agencies. There is broad agreement that all of this regulatory information has legitimate and beneficial uses. There is much less agreement on how much or, indeed, whether to share some of the information because of concerns about confidentiality, liability, and the potential for inappropriate use of some of the information.

In most cases, completed disciplinary or enforcement actions are public information. Despite their public nature, they may not be easily or conveniently available to all regulators for every person requiring a background check for employment in a financial institution. A network or system for routinely sharing this information would facilitate such checks. Other types of regulatory information would also be useful to other regulators for background checks and for identifying and investigating fraud and other financial crimes. However, regulators' willingness to share this more sensitive information will depend on resolving existing concerns.

Nevertheless, even a system for routinely sharing completed enforcement actions would increase regulatory efficiency and effectiveness in

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

conducting background investigations that could limit the migration of undesirable people, or rogues, from one financial services industry to another. To improve this process, financial regulators need the ability to readily identify individuals that have had a problematic history within the financial services sector and review the specific circumstances on a case-by-case basis. Currently, financial regulators largely depend on the self-reported information disclosed by applicants during chartering or licensing approval activities to gather information about an individual's participation and background in other financial industry.

Financial regulators should seek to validate the self-reported information on an individual's work history and confirm their reported disciplinary history. If a regulator knows an applicant has worked in another financial industry, it may currently communicate with another regulator depending on the existence of a bilateral information sharing arrangement. However, if individuals with an employment history and involvement in another financial industry do not disclose their backgrounds, it may be difficult for regulators to detect. Without an effective way of routinely checking the regulatory records of multiple industries and agencies throughout the financial services sector, some rogues are undoubtedly able to avoid being detected by regulators.

Our discussions with financial regulators revealed that disciplinary history data would be most useful when evaluating applicants seeking to enter a particular financial services industry or when conducting an investigation. Regulators routinely evaluate new industry applicants when chartering a new institution. During chartering approval activities, the regulatory body assesses the backgrounds of the directors, officers, and owners of the proposed financial institution. Similarly, new industry applicants in insurance, securities, and futures are evaluated as regulators license or

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

register those that wish to sell financial services products (e.g., agents, brokers, etc.). Financial regulators also mentioned that regulatory history data from other financial industries could be useful during investigative or enforcement activities. An ability to identify associations and linkages among both individuals and institutions would facilitate these investigative functions.

Although regulators generally share information with other regulators when asked, they may not routinely share regulatory data with each other because no convenient method for such sharing exists. Information systems and databases that could be used to conduct regulatory history checks are generally accessible to regulators within a particular financial services industry, such as within the banking or insurance industries, but may not be available or easily accessible across different financial industries. Some regulators, recognizing a need to share regulatory data with other financial regulators, have established bilateral information sharing arrangements to access external regulatory information. Using such arrangements, some regulators already access some systems and databases operated by other financial regulators. For instance, NASDR has provided some banking and futures regulators the ability to access CRD. However, even when such information-sharing agreements exist, obtaining regulatory history data from multiple financial regulators currently requires separate inquiries to each financial regulator from which such information is desired.

Regulators Need Access to Nationwide Criminal History Data

For most financial services regulators, performing routine criminal history background checks is another requirement in carrying out licensing or chartering responsibilities. Currently, financial services regulators do not all have the same ability to access criminal history information on individuals. As noted in our recent report on regulatory weaknesses

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

associated with a fraud perpetrated in the insurance industry, we found that many state insurance regulators do not have the means to routinely conduct nationwide criminal background checks on applicants who enter the industry. In contrast, the securities, futures, and banking regulators we contacted are authorized to routinely request criminal history checks on industry applicants through the FBI and other law enforcement agencies. As we noted in our earlier work, we believe insurance regulators need to have this capability to help prevent criminals from entering the industry. Representatives from NAIC and the FBI have been working on solutions to facilitate insurance regulators' ability to conduct routine criminal background checks through the FBI utilizing their recently developed automated fingerprint identification system.

FBI and regulatory officials agreed that facilitating information sharing between law enforcement and regulatory agencies was of mutual benefit. FBI officials noted that recent financial modernization efforts will make it increasingly important to assess regulatory information from all financial industries. Likewise, financial regulators may benefit from other law enforcement information beyond that typically supplied through criminal history background checks. Questions remain on the appropriate timing and extent to which information about an ongoing criminal investigation could be shared between law enforcement and regulatory agencies in a more automated fashion.

Challenges and Observations for Implementing a Shared Regulatory Data Network

Generally speaking, the concerns that financial regulators expressed to us about sharing more regulatory information with one another were not technological in nature; rather, they involved issues about the need to protect sensitive regulatory data that may be disseminated to a wider audience. These concerns include questions about what specific

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

regulatory information may be appropriate to share, the types of entities that would have access to such data, and liability issues surrounding the release of unsubstantiated information. Some of the financial regulators with whom we spoke, including SEC and NAIC, were already considering or recommending legislative remedies to facilitate enhanced information sharing with other regulators or the FBI. Because the views we obtained from regulatory agency officials were preliminary in nature and not official agency positions, we must defer to the financial regulators to convey their specific proposals or positions. Undoubtedly, legislative actions will be needed to address issues related to the sharing of sensitive information. Ultimately, the optimal implementation approach will depend on the extent to which protections are in place to make financial regulators feel comfortable in sharing sensitive regulatory information with one another.

As mentioned earlier, financial regulators possess regulatory data of varying levels of sensitivity. The financial regulators we contacted did not express concern about sharing basic regulatory history data on closed disciplinary or enforcement actions. The majority of such information is already publicly available, although not necessarily easily accessible. Such information could convey whether an individual was registered in a particular financial industry and any closed regulatory actions tied to the individual's activities in that industry. The threshold of concern rises as the sensitivity of the regulatory data rises, particularly when unsubstantiated regulatory and ongoing investigation data is involved. For example, several financial regulators pointed out that the untimely release of information on an open investigation could jeopardize that investigation and existing sources of information.

Another concern was the release of regulatory data to entities or individuals without regulatory authority. Financial regulators in both the

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

banking and securities industry believed that NAIC's status as a nonregulatory entity was a barrier to releasing regulatory data to it, even though NAIC operates on behalf of state insurance regulators. Also, some financial regulators expressed concern over the varying degrees to which individual states are obligated to protect regulatory information and the different degrees of protection that could result as such information is released among regulators.

Regulators also expressed concern with regard to the potential liability associated with disclosing some of the information maintained in their databases. Financial regulators noted that some of their regulatory data are self-reported or otherwise unsubstantiated. Release of unsubstantiated information, particularly with regard to customer complaints and open investigations, raises liability concerns for some regulators. Those regulators noted that the appropriate sharing and use of this sensitive data must be considered because of its highly prejudicial nature and the potential detriment to the party in question.

Some regulators also questioned whether the proposed system would violate the Privacy Act's prohibition against the nonconsensual disclosure of personal information contained in records maintained by federal agencies. While there are numerous exemptions to this prohibition, including the "routine use" exemption,⁷ those regulators cautioned that the Privacy Act, and its goal of safeguarding individual privacy, should be a consideration.

⁷ The routine use exemption permits nonconsensual disclosure of personal information when the internal use of the information that is disclosed is compatible with the purpose for which it was originally collected.

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

Concerning the method for facilitating the sharing of information across financial industries, the regulators we contacted generally agreed that some limited information-sharing capabilities would be useful. Most generally supported an approach whereby regulators would share some basic regulatory information on individuals, such as whether or not they were registered in another financial industry and had a disciplinary related record. However, all of the financial regulators emphasized that maintaining a centralized database containing all of the regulatory data of each financial industry would be costly and difficult to maintain. They pointed out that the vast majority of applicants were not likely to have come with a blemished regulatory history from another financial services industry. Nevertheless, most financial regulators appeared to support the concept of an information-sharing approach that would flag problems disclosed by regulators in connection with an individual's activities in other financial services industries.

A needs assessment would need to be conducted to determine the data elements most useful to each of the financial regulators and the extent to which each regulatory authority is obligated to safeguard the data it collects from its industry. In doing so, a key issue will be balancing one regulator's "need to know" with another's need to safeguard or restrict confidential or sensitive regulatory information. As an information-sharing approach is implemented and the sharing of regulatory data becomes more routine, we believe that regulators will be better positioned to predict, recognize, and reduce the movement of rogues from one industry to another. Moreover, better and more consistent information sharing may facilitate joint efforts to investigate and prosecute fraudulent behavior in the financial services industries.

Financial Services Regulators: Better Information Sharing Could Reduce Fraud

In conclusion, we have long advocated better information sharing among financial regulators and commend the Subcommittees for moving forward with its efforts to better protect consumers by improving regulators' ability to detect fraud. However, difficult issues must be addressed in order to make this a reality, and regulators will have to overcome some level of inertia and resistance to change. The Subcommittees' continued endorsement and encouragement for improvement in the inter-industry sharing of regulatory and criminal information will provide an important impetus to succeed.

Subcommittee Chairs, this concludes my prepared statement. I would be pleased to respond to any questions you or other Members of the Subcommittees may have.

Contacts and Acknowledgements

For further contacts regarding this testimony, please contact Richard J. Hillman, Director, Financial Markets and Community Investment, (202) 512-8678. Individuals making key contributions to this testimony included Lawrence D. Cluff, Barry A. Kirby, Tamara Cross, Dave Tarosky, James Black, Roger Kolar, Angela Pun, Rosemary Healy, and Shirley Jones.

(250020)