

FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF INSPECTOR GENERAL

Semiannual Report to the **Congress**



★ ★ ★ ★ ★ **April 1, 2007 – September 30, 2007** ★ ★



Including the Office of Inspector General's Performance Report for Fiscal Year 2007



The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and confidence in the nation's banking system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 4,560 individuals within seven specialized operating divisions and other offices carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured \$4.23 trillion in deposits for 8,626 institutions, of which the FDIC supervised 5,210. The Corporation held insurance funds of \$51.2 billion to ensure depositors are safeguarded.

FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF INSPECTOR GENERAL

Semiannual Report to the **Congress**



★ ★ ★ ★ ★ April 1, 2007 – September 30, 2007 ★



Inspector General's Statement

I am pleased to present the results of my office for the period April 1, 2007 –September 30, 2007. Our Fiscal Year 2007 Performance Report is also included as part of this semiannual report to show our progress in meeting annual performance goals.

During the past 6 months, we issued 12 audit and evaluation reports to management. Among those, in accordance with the Federal Information Security Management Act (FISMA), we reported the results of our review of the Corporation's information security program and practices. We noted that the Federal Deposit Insurance Corporation (FDIC) had made significant progress in recent years in addressing information security provisions of the FISMA and the National Institute of Standards and Technology, but we outlined steps that the Corporation could take to strengthen controls in certain priority areas. As is the practice in the Inspector General community, our Office of Audits (OA) was also subject to a peer review, and those results were positive. The Department of State Office of Inspector General (OIG) conducted the review and issued an unmodified opinion, indicating that OA had designed its system of quality control in accordance with standards

established by the Comptroller General and complied with the system of quality control to provide reasonable assurance of conforming to Government Auditing Standards and OA policies and procedures.

Our Office of Evaluations issued several reports and continued its efforts to provide management consulting services by conducting several management-requested assignments. One such assignment related to the Corporation's classification of costs in its New Financial Environment system, and another examined risk designation levels for the Corporation's information technology staff. At the end of the reporting period, the Evaluations group was embarking on a comprehensive assignment requested by the Chairman of the FDIC related to information technology procurement and governance practices.

We achieved many successful outcomes from our investigations over the past 6 months, and are reporting over \$40 million in total fines, restitution, and monetary recoveries. Several significant mortgage fraud cases that my office undertook in partnership with the Federal Bureau of Investigation and U.S. Attorneys' Offices resulted in stiff penalties for the offenders. To illustrate, in a case

Table of Contents

that was referred to us by the FDIC Division of Supervision and Consumer Protection in Atlanta, involving a complex \$11 million fraud scheme, the former senior vice president of nBank, Commerce, Georgia, was sentenced to 97 months of incarceration. Two mortgage brokers were also sentenced—one to 51 months and the other to 41 months of incarceration for their role in the fraud. In another case involving securities fraud, a former Wall Street executive and a co-conspirator were sentenced in a \$12 million bank securities fraud conspiracy. They were sentenced to 24 months and 18 months of incarceration, respectively, and were ordered to pay back nearly all of that amount as restitution to the government.

Given the growing investigative caseload that we are handling and the benefits that we derive from our close working relationships with the Corporation, I determined that it would be in the FDIC’s best interest to expand the OIG’s investigative presence, with a goal toward establishing offices within each Division of Supervision and Consumer Protection region. Our investigative agents are currently located only in Washington, D.C. headquarters, Atlanta, Dallas, and Chicago. I am confident that

aligning our resources in this fashion will strengthen our collaborative efforts and greatly benefit the public, the banking industry, and the FDIC.

Our vision is to be a quality-focused FDIC team that promotes excellence and trust in service to the Corporation and the public interest. I am grateful for the support that we receive from the Chairman, the Vice Chairman, and other senior leadership at the FDIC as we make that vision a reality. We are also engaged in productive dialogue with congressional staff regarding our ongoing and planned work and appreciate their feedback and interest in our office. Similarly we benefit from the experiences of our colleagues in the Inspector General community, as evidenced by a recent Best Practices Exchange that we attended at the Tennessee Valley Authority OIG and by our coordination with the OIGs of the Board of Governors of the Federal Reserve System, Department of the Treasury, and National Credit Union Administration in sponsoring an Emerging Issues Symposium here at the FDIC in November that will focus on issues that challenge us all.

Finally, I congratulate FDIC OIG Special Agents John Lucas and Patrick Collins. Along with Financial Crimes Specialist Steven Hall, an FDIC

colleague from the Division of Resolutions and Receiverships in Dallas; several Special Agents from the Federal Bureau of Investigation; and two Assistant U.S. Attorneys; John and Patrick recently received an Award for Excellence from the Inspector General community. Their outstanding efforts culminated in the prosecution of three individuals whose fraud scheme resulted in the failure of Universal Federal Savings Bank, Chicago, Illinois. The successful results of this white-collar crime case came about because of the dedication of a number of individuals from different agencies determined to work together to protect the integrity of the nation’s banking system. They can take great pride in that accomplishment.

Jon T. Rymer
Inspector General
October 31, 2007

Inspector General’s Statement	3
Abbreviations and Acronyms	6
Highlights and Outcomes	7
Strategic Goal Areas	
Supervision: Assist the FDIC to Ensure the Nation’s Banks Operate Safely and Soundly	11
Insurance: Help the FDIC Maintain the Viability of the Insurance Funds	29
Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy.....	34
Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships	39
Resources Management: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, Information Technology, and Physical Resources	43
OIG Internal Processes: Build and Sustain a High-Quality OIG Work Environment	51
Fiscal Year 2007 Performance Report	57
Reporting Requirements	64
Information Required by the Inspector General Act of 1978, as amended	65
Farewells	71
Congratulations	72

Abbreviations and Acronyms

APP	annual performance plan
BSA	Bank Secrecy Act
CACI	CACI Dynamic Systems, Inc.
COBIT®	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations
CRA	Community Reinvestment Act
DE	Dedicated Examiner
DIT	Division of Information Technology
DRR	Division of Resolutions and Receiverships
DSC	Division of Supervision and Consumer Protection
ECU	Electronic Crimes Unit
FBA	federal banking agencies
FBI	Federal Bureau of Investigation
FCB	First Citizens Bank
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
FRB	Board of Governors of the Federal Reserve System
GPRA	Government Performance and Results Act of 1993
HMDA	Home Mortgage Disclosure Act
ILC	industrial loan company
IPO	initial public offering
ITAS	Information Technology Application Services
IT	Information Technology
LIDI	Large Insured Depository Institutions
NSC	NSC Servicing
OA	Office of Audits
OCC	Office of the Comptroller of the Currency
OE	Office of Evaluations
OERM	Office of Enterprise Risk Management
OFAC	Office of Foreign Assets Control
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
PAR	performance and accountability report
PCIE	President's Council on Integrity and Efficiency
PIA	privacy impact assessments
PII	personally identifiable information
SCS	San Clemente Securities, Inc.
SNC	shared national credit
TSP	technology service provider
UCC	United Custodial Corporation

Highlights and Outcomes



The OIG's 2007 *Business Plan* contains five strategic goals that are closely linked to the FDIC's mission, programs, and activities, and one that focuses on the OIG's internal business and management processes. These highlights show our progress in meeting these goals during the reporting period. A more in-depth discussion of OIG audits, evaluations, investigations, and other activities in pursuit of these goals follows.

Strategic Goal 1 Supervision: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly

Our work in helping to ensure that the nation's banks operate safely and soundly takes the form of audits, investigations, evaluations, and extensive communication and coordination with FDIC divisions and offices, law enforcement agencies, other financial regulatory OIGs, and banking industry officials. During the reporting period, we continued work on the FDIC's evaluation of institution compliance with the anti-money laundering and terrorist financing provisions of the USA PATRIOT Act. We are also auditing examination procedures for assessing controls to protect customer and consumer information at multi-regional data processing servicers.

With respect to investigative work, as a result of cooperative efforts with U.S. Attorneys throughout the country, numerous individuals were prosecuted for financial institution fraud, and we achieved successful results in combating a number of mortgage fraud schemes. Particularly noteworthy results include the stiff sentencing of the former senior vice president of mortgage operations at nBank and two mortgage brokers for defrauding the bank. In another case, a defendant was convicted in an \$11 million mortgage loan fraud in New York. Another of our investigations led to the convictions of a former Wall Street executive and a co-conspirator in a \$12 million securities fraud conspiracy. These individuals were ordered to pay back nearly all of that amount in restitution to the government. The Office of Investigations also continued its close coordination and outreach with the Division of Supervision and Consumer Protection (DSC), the Division of Resolutions and Receiverships (DRR), and the Legal Division by way of attending quarterly meetings, regional training forums, and regularly scheduled meetings with DSC and the Legal Division to review Suspicious Activity Reports and identify cases of mutual interest. (See pages 11-28.)



Strategic Goal 2

Insurance: Help the FDIC Maintain the Viability of the Insurance Funds

Audit work related to the FDIC's dedicated examiner program confirmed that the Corporation's Dedicated Examiner Program is contributing to the FDIC's efforts to assess and quantify the risks posed by large institutions to the Deposit Insurance Fund. Given that the FDIC is not generally the primary federal regulator for the largest financial institutions, this program has placed dedicated examiners in the six largest insured depository institutions to work in cooperation with primary supervisors and bank personnel to obtain real-time access to information about the risk and trends in those institutions. Similarly, we reported positive results related to the Shared National Credit program, an interagency program to provide periodic credit risk assessment of large, complex credits held or agented by supervised institutions. (See pages 29-33.)

Strategic Goal 3

Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy

Audits and investigations contributed to the FDIC's protection of consumers in several ways. We issued a report on the FDIC's assessment of institutions' compliance management systems, reporting that FDIC examiners had adequately assessed the key components of institution compliance management systems—the board of directors and management oversight, the compliance program, and periodic compliance audits.

From an investigative standpoint, our Electronic Crimes Unit responded to Internet-based schemes where the FDIC and OIG Web sites were misused to entice consumers to divulge personal information and successfully shut down a Web site used for such purposes. The Electronic Crimes Unit was also successful in working with the Corporation to deactivate Web sites involving fraudulent claims of FDIC insurance or affiliation. (See pages 34-38.)

Strategic Goal 4

Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

We completed an assignment to evaluate the design and implementation of selected controls established by DRR to safeguard sensitive information collected and maintained in electronic form in resolution and receivership activities at FDIC-insured institutions. We made four recommendations to address vulnerabilities, and the Corporation took prompt action in response. We also continued to monitor the FDIC's Strategic Readiness Project. We continued to pursue concealment of assets investigations related to the more than \$1.7 billion in criminal restitution that the FDIC is owed. In connection with one such case, during the reporting period a debtor made a restitution payment of more than \$348,000. (See pages 39-42.)

Strategic Goal 5

Resources Management: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

Of note with respect to this strategic goal, we issued the results of our review of the FDIC's information security program and practices, in accordance with the Federal Information Security Management Act (FISMA). Our report notes strength in the areas of information security governance, incident response, and awareness training. It also identifies steps the Corporation can take to strengthen security controls in the priority areas of access control; identification and authentication; certification, accreditation, and security assessments; risk assessment; personnel security; and audit and accountability. In a related FISMA product, we reported that the FDIC continues to take action to safeguard its personally identifiable information and related systems. We issued several audit and evaluation reports in this goal area and made suggestions to improve the information technology (IT) application services contracting process and recommendations to enhance the FDIC's performance measurement processes.

We also promoted integrity in FDIC internal operations through ongoing OIG Hotline referrals, investigations of employee cases, and coordination with the FDIC's Ethics Office. (See pages 43-50.)

Strategic Goal 6
OIG Internal Processes: Build and Sustain a High-Quality OIG Work Environment

We continued to focus on a number of activities in this goal area during the past 6 months. We encouraged individual growth through professional development by way of initiatives such as training and development and career development plans for OIG staff, expanding the OIG mentoring program, and offering opportunities for OIG staff to attend graduate schools of banking. We also strengthened human capital management and leadership development by implementing end-of-assignment feedback mechanisms for staff, disseminating information on leadership training and development, and updating the OIG's business continuity and emergency preparedness plans and procedures. Our office continued to foster positive stakeholder relationships by way of OIG executives' meetings with FDIC executives; presentations at Audit Committee meetings; congressional interaction; and coordination with financial regulatory OIGs, other members of the Inspector General community, other law enforcement officials, and the Government Accountability Office. Members of the OIG Employee Advisory Group continued their quarterly meetings with the Inspector General, and we maintained and updated the OIG Web site to provide easily accessible information to parties interested in our office and the results of our work.

Our Office of Audits underwent a peer review conducted by the Department of State OIG, and our Office of

Investigations conducted internal quality control reviews of the Chicago and Dallas Office investigative operations. Office of Audits continued its work to revise audit policies and procedures to address changes in the 2007 revision to Government Auditing Standards and process changes resulting from an internal assignment management review. To ensure cost-effective and secure IT, we continued to coordinate closely with the FDIC's Division of Information Technology. We completed a laptop replacement project in OIG headquarters and field offices. We also continued to refine the OIG's training system and updated the OIG's internal Business Plan 2007 Dashboard to capture progress on achievement of strategic and performance goals. (See pages 51-56.)

Significant Outcomes	
<i>(April 2007 - September 2007)</i>	
Audit and Evaluation Reports Issued	12
Nonmonetary Recommendations	7
Investigations Opened	25
Investigations Closed	23
OIG Subpoenas Issued	7
Judicial Actions:	
Indictments/Informations	40
Convictions	22
Arrests	21
OIG Investigations Resulted in:	
Fines of	\$113,300
Restitution of	\$5,182,759
Asset Forfeiture of	\$35,073,434
Other Monetary Recoveries of	\$348,314
Total	\$40,717,807
Cases Referred to the Department of Justice (U.S. Attorney)	30
Cases Referred to FDIC Management	1
OIG Cases Conducted Jointly with Other Agencies	113
Hotline Allegations Referred	97
Proposed Regulations and Legislation Reviewed	3
Proposed FDIC Policies Reviewed	17
Responses to Requests and Appeals under the Freedom of Information Act	2



Strategic Goal 1:
Supervision: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly


Bank supervision is fundamental to the FDIC's efforts to ensure stability and public confidence in the nation's financial system. As of September 30, 2007, the FDIC was the primary federal regulator for 5,210 FDIC-insured, state-chartered institutions that were not members of the Board of Governors of the Federal Reserve System (FRB) (generally referred to as "state non-member" institutions). The Department of the Treasury (the Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS)) or the FRB supervise other banks and thrifts, depending on the institution's charter. The Corporation also has back-up examination authority to protect the interests of the deposit insurance fund for more than 3,416 (as of June 30, 2007) national banks, state-chartered banks that are members of the FRB, and savings associations.

Another important aspect of the FDIC's supervisory responsibilities relates to industrial loan companies (ILCs). The FDIC is the primary federal regulator for a number of ILCs, which are limited-charter depository institutions. ILCs may be owned by commercial firms and these parents may not be subject to consolidated supervision by a federal banking

regulator. The FDIC must establish and maintain effective controls in its processes for granting insurance to, supervising, and examining ILCs, taking into consideration the relationship between the ILC and its parent company and the effect of such a relationship on the ILC. This is especially important when the ILC's parent company is not subject to the scope of consolidated supervision, consolidated capital requirements, or enforcement actions imposed on parent organizations subject to the Bank Holding Company Act.

In recent years, the banking industry has been marked by consolidation, globalization, and the development of increasingly complex investment strategies available to banks. Bank regulators, both domestically and internationally, have devised new standards for bank capital requirements commonly referred to as Basel IA and Basel II. The FDIC and the other bank regulators continue to assess the potential impact of new standards on bank safety and soundness.

The FDIC has adopted a risk-focused approach to examining financial institutions to minimize regulatory burden and direct its resources to those areas that carry the greatest potential



risk. The FDIC must also ensure that financial institutions have adequate corporate governance structures relative to the bank's size, complexity, and risk profile to prevent financial losses and maintain confidence in those entrusted with operating the institutions. The FDIC's follow-up processes must be effective to ensure institutions are promptly complying with supervisory actions that arise as a result of the FDIC's examination process.

The Corporation is also faced with developing and implementing programs to minimize the extent to which the institutions it supervises are involved in or the victims of financial crimes and other abuse. Increased reliance by both financial institutions and non-financial institution lenders on third-party brokers has also allowed opportunities for increased real-estate frauds, including property flipping and other mortgage frauds. Examiners must be alert to the possibility of such fraudulent activity in financial institutions—it is purposeful and often hard to detect.

Part of the FDIC's overall responsibility and authority to examine banks for safety and soundness is the responsibility for examining state-chartered non-member financial

institutions for compliance with the Bank Secrecy Act (BSA). The BSA requires financial institutions to keep records and file reports on certain financial transactions. FDIC-supervised institutions must establish and maintain procedures to ensure and monitor compliance with BSA requirements. An institution's level of risk for potential money laundering determines the necessary scope of the BSA examination. In a related vein, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) promulgates, develops, and administers economic and trade sanctions such as trade embargoes, blocked assets controls, and other commercial and financial restrictions under the provisions of various laws. Generally OFAC regulations prohibit financial institutions from engaging in transactions with the governments of, or individuals or entities associated with, foreign countries against which federal law imposes economic sanctions. Sanctions can also be used against international drug traffickers, terrorists, or foreign terrorist organizations, regardless of national affiliation.

In its role as supervisor, the FDIC also analyzes data security threats, occurrences of bank security breaches, and incidents of electronic

crime that involve financial institutions. Misuse and misappropriation of personal information have emerged as major developments in financial crime. Despite generally strong controls and practices by financial institutions, methods for stealing personal data and committing fraud with that data are continuously evolving.

The OIG's role under this strategic goal is conducting audits and evaluations that review the effectiveness of various FDIC programs and examination processes aimed at providing continued stability to the nation's banks. Another major means of achieving this goal is through investigations of fraud at FDIC-supervised institutions; fraud by bank officers, directors, or other insiders; fraud leading to the failure of an institution; fraud impacting multiple institutions; and fraud involving monetary losses that could significantly impact the institution.

To assist the FDIC to ensure the nation's banks operate safely and soundly, the OIG's 2007 performance goals were as follows:

- Protect and ensure the effectiveness and efficiency of the FDIC's Supervision Program, and

- Assist FDIC efforts to detect and prevent BSA violations, money laundering, terrorist financing, fraud, and other financial crimes in FDIC-insured institutions.

OIG Work in Support of Goal 1

The OIG's Office of Audits had several audits ongoing at the end of the reporting period in the Supervision area in furtherance of our safety and soundness-related goal. These included a limited review of the FDIC's oversight of subprime credit card lending at FDIC-supervised institutions. Subprime lending refers to programs that target borrowers with weakened credit histories typically characterized by payment delinquencies, previous charge-offs, judgments, or bankruptcies. Over the years, subprime lending volumes have increased significantly. We intend to issue a memorandum providing our observations on subprime credit card lending activities.

Another assignment in this area relates to implementation of the USA PATRIOT Act. We conducted audit work to determine whether examination procedures are designed to evaluate institution compliance with the anti-money laundering and terrorist financing provisions of the Act and

whether those procedures are fully and consistently implemented to provide reasonable assurance that institutions with weak programs for detecting money laundering and terrorist financing activity will be identified and appropriate corrective measures imposed.

Other work is focusing on the FDIC's assessment of commercial real estate concentration risk, the Division of Supervision and Consumer Protection's (DSC) examination assessment of interest rate risk, and examination procedures for assessing controls to protect customer and consumer information at multiregional data processing servicers. We will report the results of these efforts in our next semiannual report.

Successful OIG Investigations Uncover Financial Institution Fraud

The OIG's Office of Investigations' work focuses largely on fraud that occurs at or impacts financial institutions. The perpetrators of such crimes can be those very individuals entrusted with governance responsibilities at the institutions—directors and bank officers. In other cases, individuals providing professional services to the banks, others working inside the bank, and

customers themselves are principals in fraudulent schemes.

The cases discussed below are illustrative of some of the OIG's success in pursuing strategic goal 1 during the reporting period. These cases reflect the cooperative efforts of OIG investigators, FDIC divisions and offices, U.S. Attorneys' Offices, and others in the law enforcement community.

Our office has investigated a number of mortgage fraud cases over the past 6 months, several of which are described below. According to the Federal Bureau of Investigation (FBI), mortgage fraud is one of the fastest growing white-collar crimes. Such illegal activity can cause financial ruin to homeowners and local communities. It can further impact local housing markets and the economy at large. Mortgage fraud can take a variety of forms and involve multiple individuals, as shown in the write-ups that follow.

Other significant cases during the reporting period involve securities fraud, obstruction of an FDIC examination, embezzlement, money laundering, and bank fraud. The OIG's success in all such investigations contributes to ensuring the continued safety and soundness of the nation's banks.

Bank Officer and Mortgage Brokers Sentenced in \$11 Million Bank Fraud on nBank

The OIG's ongoing investigation of mortgage fraud schemes orchestrated by multiple subjects operating in Georgia, Florida, Texas, South Carolina, North Carolina, and Nevada has resulted in stiff penalties for the offenders. We initiated the following investigation based on a referral from DSC's Atlanta Regional Office. Several

FDIC-regulated institutions have been victimized in these mortgage fraud schemes.

On August 9, 2007, the former senior vice president of mortgage operations at nBank, an OCC-regulated institution in Commerce, Georgia, was sentenced in the U.S. District Court for the Northern District of Georgia to 97 months of incarceration, to be followed by 3 years of supervised release. A

restitution hearing will be scheduled at a later date. In December 2006, the former senior vice president was charged and pleaded guilty to a one-count criminal information charging him with defrauding nBank of between \$7.5 and \$11 million.

In a related action, on August 17, 2007, two mortgage brokers and their companies were sentenced in the Northern District of Georgia. One of the mortgage brokers, also a co-owner of Southern Lenders Mortgage Corporation (Southern Lenders), Newman, Georgia, was sentenced to 51 months of incarceration, 3 years of supervised release, and was ordered to pay restitution in the amount of \$3.5 million. Southern Lenders was sentenced to 5 years of probation and also ordered to pay restitution in the amount of \$3.5 million. In December 2006, the mortgage broker and his company, Southern Lenders, pleaded guilty to one count of bank fraud for their role in defrauding nBank of approximately \$3.7 million.

To carry out the fraud, this first mortgage broker, acting on behalf of Southern Lenders, submitted and received short-term funding for 34 loans totaling approximately \$3.7 million from nBank. These 34 loans were placed on Southern Lenders' Warehouse line of credit at nBank. The loans were subsequently sold by Southern Lenders to several investors on the secondary market. In the normal course of business, when such loans are sold, the investors would wire the loan proceeds, and the bank would have

"This case involved the defrauding of a federally insured bank by various mortgage brokers, aided by an insider who was an officer at the bank. The integrity of the banking system and soundness of the lending industry is of importance to all citizens. Along with the FBI and the Office of Inspector General for the FDIC, we will investigate and prosecute major frauds against our federally insured banking system."

United States Attorney David E. Nahmias

received the proceeds directly from the investors. However, with the knowledge and consent of the former senior vice president of mortgage operations at nBank, the end investors, at the direction of the mortgage broker, wire transmitted the loan proceeds to a bank account in the name of the mortgage broker, doing business as J.P. Enterprises.

On the same date, another mortgage broker acting on behalf of Infinity Mortgage, also licensed in the state of Georgia, was sentenced to 41 months of incarceration and 3 years of supervised release. Infinity Mortgage was sentenced to 4 years of probation. The amount of restitution has yet to be determined. In December 2006, this second mortgage broker and his company, Infinity Mortgage, also pleaded guilty to one count of bank fraud for their role in defrauding nBank of approximately \$1.8 million in a mortgage fraud scheme.

This second mortgage broker, acting on behalf of Infinity Mortgage, submitted and received short-term funding for 23 loans totaling approximately \$1.835 million from nBank. These 23 loans were placed in Infinity Mortgage's Warehouse line of credit at nBank. The loans were to stay on the nBank line for a short period of

time while the mortgage broker found qualified investors to purchase the loans.

The mortgage broker was unable to find qualified investors to purchase the 23 loans, and the loans became aged on the nBank books. In order to remove the aged loans from the line of credit, the mortgage broker, again with the knowledge and at the direction of the former senior vice president of mortgage operations at nBank, submitted 23 new loan packages that contained false and fraudulent information. The mortgage broker's "rolling" of the loans allowed nBank to remove the aged loans from its books; however, the 23 new loans eventually were found to be fraudulent loans and nBank wrote them off. The senior vice president knew of and participated in this "rolling" scheme with the mortgage broker and several other mortgage lenders.

nBank was a national bank regulated by the OCC. The FDIC declared nBank critically undercapitalized in June 2006. In July 2006, the OCC issued a Prompt Corrective Action letter to nBank. In response to OCC's letter, nBank sold several branch locations to raise capital. nBank was unable to raise sufficient capital to continue operations, and in June 2007,

after being in business for over 103 years, nBank ceased operations after selling its remaining net assets.

Joint investigation by the FDIC OIG and FBI; prosecuted by the U.S. Attorney's Office for the Northern District of Georgia.

Conviction in \$11 Million Mortgage Loan Scheme

On September 7, 2007, in the U.S. District Court for the Eastern District of New York, one of the nine defendants in an on-going alleged scheme to defraud financial institutions of more than \$11 million in fraudulent mortgage loans pleaded guilty to conspiracy to commit bank fraud. The subject mortgage loans were initiated through New Generation Funding, LLP, (New Generation) and Exoro Funding. The defendant was previously indicted on charges of bank fraud and conspiracy to commit bank fraud. According to the indictment, the defendant presented false identification documents in March 2006 to purchase property located in Jamaica, New York. The defendant was arrested along with eight other men by FBI and FDIC OIG Special Agents on April 25, 2007.

New Generation and Exoro Funding are mortgage brokers with offices in

Queens, New York. The subject loans were funded by Fremont, Long Beach Mortgage, Argent Mortgage, BNC Mortgage, Lehman Brothers Bank, Webster Bank, Aurora Loan Services, HSBC Bank, New Century Mortgage, WMC Mortgage Corporation, American Home Mortgage, Alliance Mortgage Banking Corporation, and Equifirst Corporation. The arrests were based on a criminal complaint alleging that the defendants participated in a mortgage fraud scheme in which straw buyers were recruited to purchase properties with false identities and false identification. Much of the information on the loan applications relating to the presumed borrowers' employment and income was false. Further, the straw buyers falsely represented that the properties they were purportedly buying were going to be their primary residences in an effort to induce the lenders to loan them 100 percent of the stated purchase price. Few, if any, payments were ever made on the subject mortgages.

The defendant admitted that he and others submitted mortgage applications to the financial institutions knowing that the applications contained false identity information, false credit information, false

employment information, and false representations that the borrowers intended to make the subject properties their primary residences. The defendant also admitted that he employed straw buyers to present false identification at property closings and to sign mortgage and real estate transfer documents under false identities.

The information also charged that the defendant was a partner in a fraudulent enterprise known as NSC Servicing (NSC). NSC held itself out as a holder and servicer of existing mortgages. As part of the scheme to defraud, NSC presented pay-off letters to mortgage lenders at several real estate closings falsely claiming to be the servicer of the mortgages on the properties being sold. The closing attorneys made the pay-off checks payable to NSC, and the defendant and others negotiated the checks and kept the proceeds. The primary lien holders on the original mortgages were never paid.

The defendant is in the United States illegally and has been in custody since his arrest. He is cooperating with the investigation. A sentencing date has not yet been set by the Court. On June 25, 2007, the grand jury indicted three of the other eight subjects previously

arrested on charges of bank fraud and conspiracy to commit bank fraud.

Joint investigation by the FBI and the FDIC OIG; prosecution is being handled by the U.S. Attorney's Office for the Eastern District of New York.

Former Wall Street Executive and Co-conspirator Sentenced in \$12 Million Bank Securities Fraud Conspiracy

On August 3, 2007, in the U.S. District Court for the District of New Jersey, a former member of the Executive Committee and Director of Research at New York-based Oppenheimer & Company, Inc. was sentenced to 24 months of incarceration, to be followed by 4 months of home confinement as part of his 3-year term of supervised release. The defendant was ordered to pay \$11 million in restitution that he agreed to forfeit to the government under the terms of his plea agreement. The defendant previously pleaded guilty to one count of conspiracy to commit securities fraud in connection with initial public offerings (IPO) involving 65 mutual banks in New Jersey, Connecticut, and across the country.

On the same date, one of the defendant's co-conspirators, a retired New York City school teacher and childhood friend, was sentenced to

18 months of incarceration to be followed by 2 years of supervised release and agreed to forfeit \$802,241 to the government. As part of his plea agreement, the co-conspirator pleaded guilty to one count of conspiracy for his role in acting as a nominee in establishing accounts at banks where depositors were defrauded. The co-conspirator admitted that he traveled around the country opening up accounts in his and the defendant's name, using the defendant's money.

The defendant admitted that he organized a complex scheme to circumvent applicable federal and state banking regulations that require mutual banks to apportion shares issued in IPOs to depositors, restrict the maximum number of shares offered to such depositors, and prevent depositors from transferring their shares to other depositors.

A mutual bank is a bank owned by depositors. The depositors are entitled to have the first opportunity to buy shares in the bank when it converts to a publicly traded company. By secretly and fraudulently amassing shares to which he was not entitled and selling them, the defendant and his co-conspirators defrauded eligible depositors and the banks of more than

\$12 million. Nearly all of that amount is being forfeited to the government by the defendants.

The defendant admitted that beginning on or about December 29, 1995 and continuing to on or about February 13, 2007, he implemented a scheme to defraud various mutual savings banks, including the FDIC-insured and regulated Provident Bank, headquartered in Jersey City, N.J., and New Haven Savings Bank (now New Alliance Bank), headquartered in New Haven, Connecticut.

The defendant also admitted that he directed his co-conspirators and others to open depository accounts at, among other banks, Provident and New Haven Savings that he identified as likely to offer its depositors shares in IPOs. Upon announcement by Provident and New Haven Savings that they were offering shares to eligible depositors, the defendant directed his co-conspirators to complete stock purchase order forms that falsely represented that they were purchasing the shares for their accounts, when, in reality, he was purchasing the shares with his own money for his own benefit.

The defendant further admitted that he directed his co-conspir-

ators to either transfer the fraudulently obtained shares to him using Ameritrade accounts, or sell the shares on the open market and wire the proceeds to him.

On September 24, 2007, in another investigation involving Provident Bank, another defendant, a graduate of Harvard Business School and an Indiana businessman, involved in a very similar scheme of secretly and fraudulently amassing shares issued in IPOs, pleaded guilty in the District Court of New Jersey to one count of conspiracy to commit securities fraud. As part of his plea agreement, this defendant agreed to forfeit to the government more than \$2.8 million representing the proceeds of his illegal activities. The defendant admitted to directing at least two others to open depository accounts at Provident Bank and other banks, that he identified as likely to offer its depositors shares in IPOs. He then directed the two others to sell the shares on the open market and wire transfer the proceeds to him.

Joint investigation by the FDIC OIG, IRS-Criminal Investigation Division, U.S. Postal Inspection Service, and the FBI; prosecuted by the U.S. Attorney's Office for the District of New Jersey - Securities and Health Care Fraud Unit.

Defendants Sentenced in Connection with BestBank Failure

On August 24, 2007, in the U.S. District Court for the District of Colorado, the former president and director of BestBank, Boulder, Colorado, was sentenced to 90 months of incarceration to be followed by 3 years of supervised release. The former chief financial officer was sentenced to 72 months of incarceration to be followed by 3 years of supervised release. The judge did not order restitution but ordered forfeitures of \$4.7 million for the former president and director and \$92,643 for the former chief financial officer.

In February 2007, these defendants and the former BestBank owner and chief executive officer and chairman of the board of directors were found guilty of 15 felony counts of fraud and conspiracy relating to BestBank's \$248 million failure in 1998. The former owner and chief executive officer and chairman of the board of directors is scheduled to be sentenced in October 2007.

In addition, on August 17, 2007, the owners of Century Financial Services, Inc. and Century Financial Group, Inc. were sentenced. The owners, who were previously found guilty of bank fraud, wire fraud, filing false

bank reports, and continuing financial crimes enterprise in connection with the 1998 failure of BestBank, were each sentenced to 10 years in prison. The judge ordered forfeitures of \$11.6 million for one of the owners and \$11.7 million for the other owner.

From 1994 through July 1998, all of these defendants jointly engaged in a business operation that made more than 500,000 BestBank credit card loans to subprime borrowers. Subprime credit card borrowers are high-risk borrowers with poor credit histories. The credit card accounts were funded by BestBank using money from depositors. BestBank attracted depositors by offering above-market interest rates. In July 1998, the bank was closed. The Colorado State Banking Commissioner and the FDIC determined that the value of the subprime credit card loans maintained as an asset on the books of BestBank was overstated because delinquent loans were fraudulently made to appear nondelinquent. BestBank's liability to its depositors exceeded the value of its other assets, making it insolvent and one of the largest bank failures in the last 10 years. Depositors' losses exceeded \$200 million. The FDIC's Bank Insurance Fund covered all depositors' losses except for \$27 million of deposits which

exceeded the \$100,000 per-account insurance limit.

Joint investigation by the FDIC OIG, the FBI, and the Internal Revenue Service Criminal Investigation Division; prosecuted by the U.S. Attorney's Office for the District of Colorado.

Former President of the Bank of Paxton Pleads Guilty to Bank Fraud and Obstruction of an FDIC Examination

On July 26, 2007, in the U.S. District Court for the District of Nebraska, the former president and loan officer of the Bank of Paxton, Paxton, Nebraska, pleaded guilty to one count of bank fraud and one count of obstructing the examination of a financial institution. The Bank of Paxton lost approximately \$3.9 million as a result of the defendant's criminal activities. The Bank of Paxton was scheduled to be closed on May 23, 2006, due to the fraud, but the bank owner recapitalized the bank and prevented the closing.

It is alleged that from on or about January 2004 to April 2006, the defendant manipulated 12 loans totaling approximately \$5 million for his benefit and the benefit of others. The loans were made with forged signatures and false financial statements. In addition, during the last two FDIC and state examinations, the defendant allegedly falsified bank

documents to conceal his fraudulent activity. Our investigation revealed that just days before the start of bank examinations, the defendant posted positive information on nonperforming loans to give the appearance that the loans were performing. Immediately after the examinations, the defendant reversed the postings. In addition, the defendant submitted false quarterly reports to the Bank of Paxton's Board of Directors to conceal his illegal activity.

He also stole \$300,000 from a wealthy Bank of Paxton bank customer. The customer was on the Board of Directors and the defendant knew that he checked his account infrequently. The defendant was able to steal money out of the customer's account and move it to his wife's account and other accounts where he maintained control.

Joint investigation by the FDIC OIG and the FBI; prosecution is being handled by the U.S. Attorney's Office for the District of Nebraska.

Former Vice President of Alliance Bank Found Guilty on Multiple Counts of Bank Fraud

In a decision reached on July 18, 2007, by a judge in the U.S. District Court for the District of Minnesota, the former vice president of Private Banking, Alliance Bank, New Ulm,

Minnesota, was found guilty of one count of conspiracy, three counts of forging securities, seven counts of embezzlement by a bank officer, and three counts of mail fraud.

The defendant was a primary lending officer at the bank's Edina branch office where she specialized in larger commercial loans and lending to borrowers of higher net worth. She was employed by the bank from July 15, 1996, until her negotiated severance on December 10, 2004. Alliance management terminated her employment based on questionable lending judgment and unauthorized lending that caused losses in excess of \$1.1 million.

According to the earlier indictment, the defendant used her position as a loan officer to divert for her own use funds that customers paid to the bank as well as fictitious fees she tricked customers into paying. The defendant converted checks received from bank customers into cashier's checks and funneled those checks into another bank account. At times, she forged check signatures and endorsements. In an attempt to conceal her embezzlement, she altered bank records and made false statements when questioned by bank employees about specific transactions. Over a 4-year

period, the defendant and two co-conspirators used the money obtained through this scheme for vacations, home renovations and decorating, automobiles, cosmetic surgery, gambling, and country club dues. In all, the defendant and her co-conspirators embezzled approximately \$1 million from the bank and its customers.

Joint investigation by the FDIC OIG and the FBI, based on a referral from DSC Kansas City Regional Office; prosecution is being handled by the U.S. Attorney's Office for the District of Minnesota.

Former Senior Vice President of Capital Bank and Trust Pleads Guilty to Bank Fraud

On July 24, 2007, the former senior vice president, Capital Bank and Trust Company (Capital), Albany, NY, waived indictment and pleaded guilty to a criminal information charging him with misapplication of bank funds.

According to the information, between 1997 and 2003, the defendant approved a series of risky loans for a number of individuals and businesses contrary to sound lending practices and in violation of Capital's own lending requirements. A number of these loans defaulted causing losses to Capital of at least \$824,270. In making these loans, the defendant, on several occasions, forged the signatures of two presidents

of Capital, which were required for the approval of the loans, and used improper bank procedures and secrecy to ensure that the loans were approved.

The defendant also stipulated to an action under 8(e) of the Federal Deposit Insurance Act, which provides for a lifetime ban from banking.

Joint investigation by the FDIC OIG, the FBI, and the Legal Division of the FDIC New York Regional Office; prosecuted by the Fraud Section of the Criminal Division of the U.S. Department of Justice.

Former Loan Officer Pleads Guilty to One Count of Bank Fraud

On June 8, 2007, a former loan operations officer at The PrivateBank and Trust Company, an FDIC-regulated institution, pleaded guilty to one count of bank fraud, as charged in an information filed in May 2007 in the Northern District of Illinois.

The information alleged that from approximately July 2000 and continuing to at least November 2006, the defendant executed a scheme to defraud The PrivateBank and Trust Company. In particular, the defendant created a fictitious line of credit for \$775,000 in the name of a customer, backdated it, and used his mother's address for the fictitious line of credit.

The defendant then took draws on the line of credit and eventually transferred the funds to his personal checking account. In addition, the defendant attempted to conceal his scheme by processing the transaction on The PrivateBank and Trust Company's internal data processing system to hide the outstanding balance on the fictitious line of credit from the bank's internal and external auditors. The result was a loss to the bank of approximately \$916,191.

Joint investigation by the FDIC OIG and the FBI; prosecution was handled by the U.S. Attorney's Office for the Northern District of Illinois.

Former VP of Operations at Burlington Bank & Trust Pleads Guilty

On August 1, 2007, the former vice president of operations, Burlington Bank & Trust, Burlington, Iowa, pleaded guilty in the U.S. District Court for the Southern District of Iowa, to a five-count information charging him with two counts of misapplication and embezzlement of bank funds and three counts of money laundering.

According to an earlier information, the defendant allegedly made 109 internal transactions causing money to be transferred to his and/or the accounts of his fiancé, now wife, from

the bank's internal expense accounts. Transactions were also initiated causing bank checks to be issued or Internet payments to be made to third parties, such as credit card companies, in payment of monies owed by the defendant and his wife. The defendant's activities account for approximately \$569,115 in losses to the bank.

As part of his plea agreement, the defendant stipulated to an action under 8(e) of the Federal Deposit Insurance Act, which provides for a lifetime ban from banking and agreed to pay restitution in the amount of \$548,889 immediately upon imposition of his sentence.

Joint investigation by the FDIC OIG and the FBI, based upon on a referral from DSC; prosecution is being handled by the U.S. Attorney's Office for the Southern District of Iowa.

Former Vice President of First Citizens Sentenced to Prison

On June 20, 2007, in the U.S. District Court for the Eastern District of North Carolina, the former Vice President, Cash Management Sales Specialist, First Citizens Bank (FCB), Raleigh, North Carolina, was sentenced to 33 months of incarceration, to be followed by 3 years of supervised release and was ordered to pay \$230,000 in restitution

to FCB. He earlier pleaded guilty in April 2007 to a criminal information charging him with one count of embezzlement.

The defendant admitted to devising a scheme to divert \$240,533 of bank funds by the creation of fictitious loans and making partial withdrawals from customers' certificates of deposit. When the defendant needed cash, he completed withdrawal slips in the customers' name and then obtained the cash (cashier's check or money order) from behind the teller line. The defendant made the negotiable instruments payable mostly to his creditors. However, on occasion, the defendant made the negotiable instruments payable to himself and deposited the funds into his personal account maintained at a non-FCB branch. Prior to entering his plea, the defendant made a repayment of \$10,000 to FCB.

Joint investigation by the FDIC OIG and the FBI; prosecuted by the U.S. Attorney's Office for the Eastern District of North Carolina.

Other Successful Outcomes

Former President of Canton State Bank and His Wife Sentenced on Multiple Charges of Bank Fraud

On August 30, 2007, the former president of Canton State Bank and

his wife, both of Lebanon, Missouri, were sentenced in the in the U.S. District Court for the Eastern District of Missouri. The former president was sentenced to 27 months in prison, to be followed by 5 years of supervised release, and was ordered to pay restitution in the amount of \$315,412. His wife was sentenced to 4 months of home confinement, to be followed by 5 years of supervised release, and was ordered to pay restitution in the amount of \$81,984. Earlier, both defendants pleaded guilty to fraud charges involving false statements to obtain nominee loans. The former president pleaded guilty to one count of making a false statement and bank fraud, and his wife pleaded guilty to one count of false statements.

As previously reported, the defendants were indicted by a federal grand jury on 26 felony counts of conspiracy to make false statements to FDIC-insured institutions and the U.S. Department of Agriculture Farm Service Agency, false statements, money laundering, and bank fraud.

Joint investigation by the FDIC OIG, the FBI, and U.S. Department of Agriculture OIG, based on a referral from DSC; prosecuted by the U.S. Attorney's Office for the Eastern District of Missouri.

★ ★ ★ ★ ★

Bank Employee Pleads Guilty to Stealing Over \$3.2 Million from BancFirst

On July 26, 2007, the former vault teller and teller supervisor at a branch office of BancFirst in Seminole, Oklahoma pleaded guilty in the U.S. District Court for the Eastern District of Oklahoma to an information charging her with one count of false entry in the books of an FDIC-insured bank and one count of criminal forfeiture. The criminal forfeiture includes a money judgment of approximately \$3,263,695; and forfeiture of real property, including 11 motor vehicles and tractors, electronic entertainment equipment, furniture, and jewelry.

The defendant admitted to creating false internal bank documents showing the movement of cash in and out of the branch vault, and then separately created false internal bank documents using the general ledger accounts to cure the account imbalances due to the initial false entries. The amount of proceeds obtained by the defendant and as a result of the offenses is approximately \$3,263,695.

Joint investigation by the FDIC OIG and the FBI; prosecution is being handled by the U.S. Attorney's Office for the Eastern District of Oklahoma.

★ ★ ★ ★ ★

Jury Finds Owners of Stardancer Casino Guilty on 28 Counts of Fraud

On May 17, 2007, after a 9-day trial in the District of South Carolina, Florence Division, the owners of Stardancer Casinos Inc. (Stardancer) of Duluth, Georgia, were found guilty by a federal jury on 28 counts of tax fraud, conspiracy to commit mail fraud, mail fraud, wire fraud, deprivation of honest services, receiving stolen property, and money laundering.

The former president and chief executive officer of Stardancer and his spouse operated casino boats in Little River, South Carolina, and several locations in Florida between February 1999 and January 2003. Upon the conclusion of the trial, the defendants were both found guilty of 18 counts of tax fraud for the period April 2001 to November 2002. Evidence presented during the trial showed the defendants were responsible for withholding employment taxes from 300 Stardancer employees' payroll checks and failed to pay those taxes to the government. The defendants also failed to pay excise taxes while operating the casino boats, resulting in a loss to the United States of approximately \$2.8 million.

The defendants were also found guilty of one count of conspiracy

to commit mail fraud, wire fraud, and deprivation of honest services. Evidence presented during the trial established that the defendants conspired to commit mail fraud from January 1999 through December 2003. The defendants purchased at least \$148,000 in personal items with credit cards and paid for those items with Stardancer Casino funds. Their scheme also involved coding those personal charges to Stardancer's general ledger as business expenses. In addition, the defendants were each charged with three counts of mail fraud for their purchase of insurance for their 56-foot Sea Ray yacht. Similar to their credit card scheme, the defendants charged their personal yacht insurance to Stardancer's general ledger as a business expense and paid for the insurance, totaling approximately \$17,500, with Stardancer funds.

The former president and chief executive officer of Stardancer was also found guilty of three counts of receiving stolen property. Evidence presented at trial established that between December 1998 and January 2002, he received 3 checks totaling approximately \$2.3 million from the Oakwood Deposit Bank Company (Oakwood), Oakwood, Ohio, knowing the funds had been stolen. He was

also found to have deposited those three checks into Stardancer's checking account at the Bank of America, knowing that those funds were derived from an ongoing embezzlement scheme at Oakwood; resulting in his conviction of three counts of money laundering. In total, between the period November 1998 and January 2002, he received approximately \$41 million in stolen funds either directly or for the benefit of Stardancer.

Upon their conviction, the defendants immediately consented to the forfeiture of \$835,000 in personally owned stock. It was determined that the stock was originally purchased from the proceeds of the defendants' personal checking accounts which had been funded by their Stardancer salaries.

The investigation into Stardancer was initiated in February 2002, when the former President of the Oakwood Deposit Bank Company, Oakwood, Ohio, confessed to embezzling over \$40 million from Oakwood Deposit Bank Company which led to the bank's insolvency. He admitted that most of the money was embezzled to Stardancer. Investigators eventually determined that approximately \$41 million was embezzled to Stardancer, and ultimately shut down the company in January 2003, with the execution

of search warrants and seizure of Stardancer's gambling vessels and shuttle craft. The former president pleaded guilty to embezzlement and money laundering and was sentenced to 14 years' imprisonment and was ordered to pay \$48,718,405 in restitution.

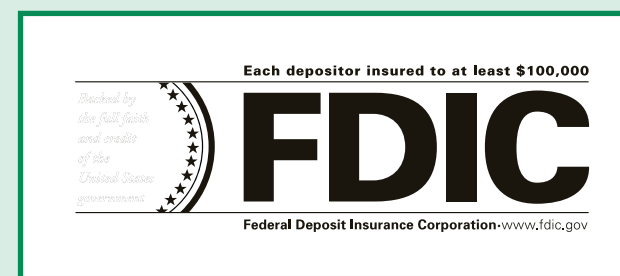
The investigation into Stardancer Casinos was conducted by the FDIC OIG, the Internal Revenue Service-Criminal Investigation Division, and the FBI. The case was prosecuted by the District of South Carolina, Florence Division, and the U.S. Department of Justice, Criminal Division, Fraud Section, Washington D.C.

A Strong Partnership

The OIG has partnered with various U.S. Attorneys' Offices throughout the country in bringing to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC, or criminally impeded the FDIC's examination and resolution processes. The alliances with the U.S. Attorneys' Offices have yielded positive results during this reporting period.

Our strong partnership has evolved from years of trust and hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the nation's financial system.

For the current reporting period, we are especially appreciative of the efforts of the Assistant U.S. Attorneys in the following offices: Eastern District of New York, Western District of Wisconsin, District of New Jersey—Securities and Health Care Fraud Unit, Middle District of Florida, Eastern District of Missouri, Northern District of Texas, Northern District of Georgia, District of Colorado, District of Nebraska, Eastern District of Kentucky, Western District of Washington, District of Minnesota, Southern District of Texas, Eastern District of North Carolina, Southern District of Illinois, District of Kansas, Eastern District of Michigan, Eastern District of Oklahoma, District of South Carolina, and the Western District of Missouri. The OIG also worked closely with Trial Attorneys from the Fraud Section of the Criminal Division of the Department of Justice.



Strategic Goal 2

Insurance: Help the FDIC Maintain the Viability of the Insurance Fund

Federal deposit insurance remains a fundamental part of the FDIC's commitment to maintain stability and public confidence in the Nation's financial system. In February 2006, President Bush signed into law the Federal Deposit Insurance Reform Act of 2005, prompting sweeping changes in the federal deposit insurance system. The Congress gave the Corporation 9 months to implement most of the provisions of the legislation. In October 2006, the FDIC Board of Directors approved a final rule to implement a one-time assessment credit to banks and thrifts. The credit is used to offset future assessments charged by the FDIC and recognizes contributions that certain institutions made to capitalize the funds during the first half of the 1990s. In November 2006, the Board also adopted a final rule on the pricing structure and approved a more risk-sensitive framework for the 95 percent of insured institutions that are well capitalized and well managed.

In addition to the extensive rulemaking required in conjunction with deposit insurance reform, fundamental changes have been made in the FDIC's business functions, including modification to major application systems and creation of new on-line tools. System changes in

support of deposit insurance reform will continue.

The continuing consolidation of the banking industry means there are a few very large institutions that represent an increasingly significant share of the Deposit Insurance Fund's risk exposure. Industry consolidation presents benefits and risks to the Deposit Insurance Fund. While the risks to the funds are diminished because of the diversification benefits of consolidation (along geographic and product lines), the concentration of deposits in fewer insured depository institutions increases the risks to the Deposit Insurance Fund in the event a large insured depository institution fails.

As a result of industry consolidation, the assets in the industry are also increasingly concentrated in a small number of large, complex institutions for which the FDIC is not, for the most part, the primary regulator. The largest banks operate highly complex branch networks, have extensive international and capital market operations, and work on the cutting edge of technologically sophisticated finance and business. The increased complexity of the industry and the concentration of risk to the insurance funds in the largest banking organizations are expected to grow more pronounced

over time and to present greater risk-management challenges to the Corporation. A two-tiered banking system characterized by a limited number of very large, complex institutions and a much larger number of small community banks has emerged. The banking regulators, including the FDIC, need insight into the risks that are inherent in these different types of banking organizations.

To help the FDIC maintain the viability of the deposit insurance fund, the OIG's 2007 performance goal was as follows:

- Evaluate corporate programs to identify and manage risks in the banking industry that can cause losses to the fund.

OIG Work in Support of Goal 2

As insurer, the FDIC needs a comprehensive understanding of the risks that the largest institutions pose to the Deposit Insurance Fund. The FDIC is not the primary federal regulator for most of the large institutions that it insures. Therefore, the risk assessment process is based on a combination of information obtained from the primary federal regulator, the institution, supervisory activities, market data, and publicly available data. The FDIC established the Large Bank Branch

in headquarters to coordinate the FDIC's nationwide programs focused on supervising and assessing risk in large institutions. A key program in this regard is the Dedicated Examiner (DE) Program, established in 2002. This program has placed dedicated examiners in the six largest insured depository institutions to work in cooperation with primary regulators and bank personnel to obtain real-time access to information about the risk and trends in those institutions. We conducted an audit to determine whether the DE Program is contributing to the FDIC's efforts to assess and quantify the risks posed by large institutions to the Deposit Insurance Fund.

Another of our audits during the reporting period assessed the FDIC's role in reviewing shared national credits (SNC) and the consideration of SNC ratings in risk management examinations of FDIC-supervised institutions. SNCs represent the largest and most complex loans and loan commitments held by FDIC-insured institutions.

Dedicated Examiner Program

By way of background, the FDIC's DSC is responsible for the FDIC's Large Insured Depository Institutions (LIDI) Program, which consists of

financial institutions with consolidated banking assets that exceed \$10 billion. At the time of our audit, there were 119 insured institutions covered by the LIDI Program, 25 of which were FDIC supervised. The 119 institutions had total assets exceeding \$9 trillion and total deposits of \$5.6 trillion, comprised of both insured and uninsured deposits. To assist the FDIC in assessing the risks associated with the largest institutions in the LIDI program that are not FDIC-supervised, the FDIC and the other federal banking agencies (FBAs) established the DE Program. The DE Program includes six LIDIs supervised by either OCC or OTS.

Our audit determined that the DE Program has been successful in providing the FDIC with supervisory information related to the operations at the six largest insured institutions and risks associated with those institutions. The DE Program has provided the FDIC with information related to those institutions' organizational and legal structures; international activities; business segments; insured deposits; various types of risks, including credit, market, and interest rate; and supervisory actions and strategies—all of which are important in assessing and mitigating risk to the DIF. FDIC


officials indicated that the DE Program has been an effective mechanism through which supervisory, insurance, and resolution-related information is obtained.

Further, the DEs have complied with DSC guidance on reporting information relative to DE Program institutions and have established effective working relationships with the institutions and their respective FBAs—OCC and OTS officials—as well as FDIC officials in the Division of Insurance and Research and Division of Resolutions and Receiverships.

Our audit report did not contain recommendations. However, DSC provided a response stating that the FDIC would continue to assess means for improving the efficiency and overall effectiveness of the LIDI and DE programs.

Shared National Credits

An SNC is defined as any loan and/or formal loan commitment extended to a borrower by a supervised institution (subject to supervision by one of the FBAs), its subsidiaries, and affiliates that totals \$20 million or more and (1) is shared by three or more insured institutions under a formal lending agreement or (2) a portion of which is sold to two or more insured institu-



tions, with the purchasing institutions assuming a pro rata share of the credit risk. An agent originates an SNC and administers it for the other lenders.

The SNC Program is an interagency program, established in 1977, to provide a periodic credit risk assessment of the largest and most complex credits held or agented by supervised institutions. The SNC Program is administered by the four FBAs: OCC, FRB, FDIC, and OTS. The FDIC's DSC is responsible for fulfilling the FDIC's role in the SNC Program.

For 2007, the SNC Program included 205 agent institutions, of which 26 were FDIC-supervised institutions, that originated about 7,700 credits with a \$2.3 trillion commitment balance. About 800 of the more than 5,200 FDIC-supervised banks participate in SNCs. For these 800 institutions, the SNC Program has the potential beneficial effects of avoiding duplicate credit reviews and ensuring consistency in rating determinations.

As a result of our audit work, we reported that the SNC Program is a well-established interagency program with appropriate interagency coordination and documentation. The FDIC has a role similar to that of the other banking agencies in providing a

periodic credit risk assessment of the largest and most complex credits held by insured financial institutions in the United States.

The FDIC uses information from the SNC Program in risk management examinations and analyses of emerging risks at large banks, including underwriting and industry performance trends. There were a total of nine sites for the 2007 SNC review where the FDIC examiners served as the Examiner-in-Charge. We reviewed three such SNC examination sites and determined that the FDIC examiners had appropriately followed guidance and that credit ratings were adequately supported by examiner working papers. According to DSC examiners, SNC results help achieve efficiencies in risk management examinations by using the SNC rating assigned to credits, thus avoiding multiple reviews of the same credits as part of individual risk management examinations of participating institutions.

Although we did not make recommendations in this report, we did identify a matter for further consideration by FDIC management involving the process used to identify SNCs that are agented by entities that are not supervised institutions (such as insurance companies and securities

firms) meaning that the institution is not subject to examination by one of the FBAs. The interagency letter sent to all known agent financial institutions each December asks these institutions to report SNCs that are agented by an entity that is not a supervised institution. However, this process is unlikely to identify those SNCs in which the agent entities are not supervised institutions. Given the benefits of the SNC Program in terms of insight into industry risk and performance and efficiencies gained in the examination process, we noted that the FDIC, together with the other FBAs, should consider assessing the need for additional guidance and controls over the identification of SNCs agented by entities that are not supervised institutions.

In response to a draft of this report, the FDIC commented that it would discuss the need for additional guidance and controls over the identification of SNCs agented by entities that are not supervised institutions with the other FBAs.

Strategic Goal 3:

Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy



Consumer protection laws are an important part of the safety net of America. The U.S. Congress has long advocated particular protections for consumers in relationships with banks. For example:

- **The Community Reinvestment Act** encourages federally insured banks to meet the credit needs of their entire community.
- **The Equal Credit Opportunity Act** prohibits creditor practices that discriminate based on race, color, religion, national origin, sex, marital status, or age.
- **The Home Mortgage Disclosure Act** was enacted to provide information to the public and federal regulators regarding how depository institutions are fulfilling their obligations towards community housing needs.
- **The Fair Housing Act** prohibits discrimination based on race, color, religion, national origin, sex, familial status, and handicap in residential real-estate-related transactions.
- **The Gramm-Leach-Bliley Act** eliminated barriers preventing the affiliations of banks with securities firms and insurance companies and mandates new privacy rules.

- **The Truth in Lending Act** requires meaningful disclosure of credit and leasing terms.
- **The Fair and Accurate Credit Transaction Act** further strengthened the country's national credit reporting system and assists financial institutions and consumers in the fight against identity theft.

The FDIC carries out its role by (1) providing consumers with access to information about their rights and disclosures that are required by federal laws and regulations and (2) examining the banks where the FDIC is the primary federal regulator to determine the institutions' compliance with laws and regulations governing consumer protection, fair lending, and community investment.

FDIC Chairman Bair has stressed the importance of economic inclusion and has expressed concern that market mechanisms are not working as well as they should for low-to-moderate income families who must often pay high amounts for basic financial services that others obtain at far less cost. Many people lack the financial skills needed to analyze and compare products and their prices. Oftentimes the problem is the lack of disclosures that describe a product and its true

costs in fair and simple terms. Another factor could be linked to aspects of safety and soundness regulation that could unnecessarily deter banks from serving the needs of their communities or create conditions that favor high-cost products. To address these concerns, in addition to the FDIC's existing Money Smart program, the Corporation has undertaken other initiatives, including creation of an Advisory Committee on Economic Inclusion. As the Chairman has pointed out, continuing dialogue among consumer advocates, regulators, and the banking industry is key to the challenge of closing the gap between what the unbanked and underbanked pay for credit and what those in the mainstream pay. In congressional testimony and other forums, the Chairman has focused on strengthening protections available to borrowers in the subprime mortgage market and ensuring that predatory lending practices do not take root in the banking system.

The OIG's role under this strategic goal is targeting audits and evaluations that review the effectiveness of various FDIC programs aimed at protecting consumers, fair lending, and community investment. Additionally, the OIG's investigative authorities are used to identify, target, disrupt,

and dismantle criminal organizations and individual operations engaged in fraud schemes that target our financial institutions.

To assist the FDIC to protect consumer rights and ensure customer data security and privacy, the OIG's 2007 Performance Goals were as follows:

- Evaluate the effectiveness of FDIC programs for ensuring customer data security and privacy at FDIC-insured institutions.
- Review FDIC's examination coverage of institution compliance at FDIC-insured institutions.
- Address allegations of fraudulent insurance coverage and identity theft schemes affecting the FDIC.

OIG Work in Support of Goal 3

We completed an audit of DSC's examination assessment of financial institutions' Compliance Management Systems (CMS) during the reporting period.

Investigative work related to protection of personal information and misrepresentation of deposit insurance also supported this strategic goal area during the reporting period, as described below.



Compliance Management Systems

Compliance examinations are the primary supervisory tool the FDIC uses to determine whether a financial institution is meeting its responsibility to comply with the requirements of federal consumer protection laws and associated regulations.

The FDIC introduced risk-scoping in the compliance examination process in the mid-1990s. In June 2003, as part of the continued focus on risk-scoping, the FDIC revised the compliance examination process to increase attention on an institution's CMS. Although not required by law or regulation, the FDIC has stated it expects the institutions it supervises to have an effective CMS designed to aid compliance with consumer protection laws and regulations. Three interdependent elements comprise a CMS: a board of directors and management oversight; a compliance program (including policies and procedures, training, monitoring, and consumer complaint response); and periodic compliance audits.

Our review of seven sampled institutions showed that the examiners had adequately assessed each financial institution's CMS as part of the related compliance examination.

Specifically, the examiners (1) completed a preliminary risk assessment that addressed each institution's CMS to assist in risk-scoping the examination and (2) documented support for examination conclusions regarding the CMS. Additionally, the Reports of Examination for the seven institutions addressed each CMS element referenced above (board and management oversight, compliance program, and compliance audits), and included a summary statement and conclusion on the quality of each financial institution's compliance management practices for each element. Also, where significant violations were identified, the examiner tied the cause of the violation to one of the CMS elements in the Reports of Examination.

The report did not make recommendations. DSC management commented that it was committed to ensuring that financial institutions implement effective consumer protection safeguards by maintaining strong CMSs.

Ongoing Audit Work

Audit work currently underway is assessing the implementation of the FDIC's supervisory guidance for nontraditional mortgage products.

That audit will assess the FDIC's efforts

to (1) identify FDIC-supervised institutions engaged in significant nontraditional mortgage lending and (2) develop supervisory plans to address risks associated with such lending.

Office of Investigations Works to Curtail Identify Theft and Misrepresentation of FDIC Insurance or Affiliation

Identity theft continues to become more sophisticated, and the number of victims is growing. Identity theft includes using the Internet for crimes such as "phishing" emails and "pharming" Web sites that attempt to trick people into divulging their private financial information. Schemers pretend to be legitimate businesses or government entities with a need for the information that is requested. The OIG's Electronic Crimes Unit (ECU) responds to such phishing and pharming scams involving the FDIC and the OIG.

Unscrupulous individuals also sometimes attempt to misuse the FDIC's name, logo, abbreviation, or other indicators to suggest that deposits or other products are fully insured. Such misrepresentations induce the targets of schemes to trust in the strength of FDIC insurance while misleading them as to the true nature of the insurance investments being offered. Abuses

of this nature harm consumers and can also erode public confidence in federal deposit insurance. Our Office of Investigations uses the ECU to counteract these abuses and also partners with others to pursue cases of this type.

Electronic Crimes Unit Success

During the reporting period, the ECU opened five new cases related to phishing involving the FDIC. In one of the new cases, the ECU was able to have the fraudulent Web site deactivated. The other four new cases involved the fraudulent use of the FDIC name or logo in an email or fax as part of a phishing scheme. In these cases, the ECU traced the schemes to locations outside of the United States and worked with the Department of Justice, Computer Crimes and Intellectual Properties Section, to notify foreign law enforcement of the fraudulent schemes using the FDIC name.

Additionally, the ECU investigated two new instances of Web sites that falsely advertised FDIC insurance. In both cases, the ECU, working with FDIC contractor Brandimensions, was able to have the sites deactivated.

In addition, the ECU provided forensic computer assistance on nine existing and three new FDIC OIG cases. The



Strategic Goal 4: Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

cases involved bank fraud at open and closed financial institutions and employee misconduct cases involving the improper use of FDIC computers. The forensic computer assistance involved the analysis of electronic evidence gathered from computers and other electronic media. The ECU typically searches the electronic evidence for key-words or phrases, searches for documents and emails and other artifacts, and recreates specialized software applications such as accounting software.

Securities Brokers Sentenced in Fraud Schemes

Also during the reporting period, three brokers were sentenced in the U. S. District Court for the Northern District of Texas. These sentencing affirm the severity of misrepresentations regarding FDIC insurance or affiliation. Two of the defendants were co-owners of San Clemente Securities, Inc. (SCS) and United Custodial Corporation (UCC), located in San Clemente, California. They were each sentenced to 60 months of imprisonment and 2 years of supervised release after earlier pleading guilty to count 57 of an 88-count indictment, which charged both defendants with mail fraud. A third broker, employed at SCS, earlier pleaded guilty to one count of misprision

of a felony and was sentenced to 4 years of supervised release.

Beginning in early June 1995 and continuing through April 2001, SCS advertised FDIC-insured certificates of deposit (CDs) at interest rates greater than those available from financial institutions. The investors' CDs were custodialized and held in the name of UCC. The defendants falsely and fraudulently failed to advise investors nationwide that SCS and UCC would subtract undisclosed fees ranging from 3 percent to 50 percent of the amount invested. They made false representations regarding FDIC insurance coverage of the CDs. The investment confirmations and statements they sent to investors were false and intentionally misleading, and money paid to investors when they liquidated an investment prior to maturity was actually money invested by another investment or by other persons. The investors had no ownership in any investment that would be purchased in UCC's name. In 1997, SCS, along with its co-owners, had been banned by the National Credit Union Administration from doing business with federally insured credit unions because of SCS's deceptive practices.

Joint investigation by the FDIC OIG and the FBI; prosecuted by the U.S. Attorney's Office for the Northern District of Texas.

The United States provides protection to depositors in its banks, savings and loan associations, and credit unions. One of the key players in this process is the FDIC. Among its various functions, the FDIC seeks the least costly option to resolve the institution and acts as the receiver or liquidating agent for failed FDIC-insured institutions. The success of the FDIC's efforts in resolving troubled institutions has a direct impact on the banking industry and on the taxpayers.

The Division of Resolutions and Receiverships (DRR) exists to plan and efficiently handle the resolutions of failing FDIC-insured institutions and to provide prompt, responsive, and efficient administration of failing and failed financial institutions in order to maintain confidence and stability in our financial system.

- The **resolution process** involves valuing a failing federally insured depository institution, marketing it, soliciting and accepting bids for the sale of the institution, determining which bid to accept and working with the acquiring institution through the closing process.
- The **receivership process** involves performing the closing function at the failed bank; liquidating

any remaining assets; and distributing any proceeds to the FDIC, the bank customers, general creditors, and those with approved claims.

The FDIC's resolution and receivership activities pose tremendous challenges. Today record profitability and capital in the banking industry have led to a substantial decrease in the number of financial institution failures compared to prior years. There were no bank failures during 2006; however as of September 30, 2007, two banks had failed: (1) Metropolitan Savings, Pittsburgh, Pennsylvania, with approximately \$15.8 million in assets and (2) NetBank, Alpharetta, Georgia, with approximately \$2.5 billion in assets and \$2.3 billion in total deposits. As indicated by the trends in mergers and acquisitions, banks are becoming more complex, and the industry is consolidating into larger organizations. As a result, the FDIC could potentially have to handle a failing institution with a significantly larger number of insured deposits than it has had to deal with in the past.

The change between how the FDIC handled resolutions and receiverships 20 years ago and how it will be handling them 20 years from now will be largely based on learning

to anticipate and plan, instead of reacting. Through the development of new resolution strategies within the various DRR business lines, FDIC must set far-reaching plans for the future to keep pace with a changing industry.

The OIG's role under this strategic goal is conducting audits and evaluations that assess the effectiveness of the FDIC's various programs designed to ensure that the FDIC is ready to and does respond promptly, efficiently, and effectively to financial institution closings. Additionally, the OIG investigative authorities are used to pursue instances where fraud contributes to a bank's failure or is committed to avoid paying the FDIC civil settlements, court-ordered restitution, and other payments as the institution receiver. The OIG continues to work with FDIC officials to keep current with ongoing efforts being taken by DRR and the Corporation as a whole, to sustain proficiency in resolution activity and to prepare for the possibility of a large institution failure or multiple failures caused by a single catastrophic event.

To help ensure the FDIC is ready to resolve failed banks and effectively manages receiverships, the OIG's 2007 performance goals were as follows:

- Evaluate the FDIC's plans and systems for managing bank resolutions.
- Respond to potential crimes affecting the FDIC's efforts to recover financial losses.

OIG Work in Support of Goal 4

DRR has the primary responsibility for resolving failed FDIC-insured institutions promptly, efficiently, and responsively to maintain public confidence in the nation's financial system. In performing their duties, DRR personnel have access to a wide variety of records containing sensitive information concerning bank employees and customers. Prior OIG work focused on DRR efforts to protect such information in hardcopy form. During the reporting period we completed an audit focusing on DRR's protection of electronic records.

DRR Protection of Electronic Records

Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding the sensitive information the FDIC collects when conducting resolution and receivership activities at FDIC-insured financial institutions. Such information

includes, for example, reports on potential financial institution failures and sensitive personally identifiable information for institution depositors, borrowers, and employees.

Much of the sensitive information handled by the FDIC falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure. These statutes and regulations include the Privacy Act of 1974; the Federal Information Security Management Act of 2002 (FISMA); and the FDIC's Rules and Regulations--Parts 309, *Disclosure of Information*, and 310, *Privacy Act Regulations*.

One of our audits this reporting period evaluated the design and implementation of selected controls established by DRR for safeguarding sensitive electronic information collected and maintained as a result of resolution and receivership activities at FDIC-insured financial institutions.

DRR had established a number of important controls to safeguard the sensitive electronic information it collects and maintains as a result of resolution and receivership activities at FDIC-insured financial institutions. However, we identified several vulnerabilities that increased the

risk of unauthorized use of sensitive information.

DRR and Division of Information Technology security officials took prompt action during our audit to better safeguard sensitive resolution and receivership information. We made four recommendations to address our concerns. The DRR Director concurred with all four recommendations.

OIG Continues to Monitor the FDIC's Strategic Readiness Project

One of the greatest risks to the Deposit Insurance Fund and public confidence in the nation's financial system would be the failure of a large bank. The FDIC has put plans in place to deal with the possibility of a large bank failure, and in that regard it undertook a Strategic Readiness Project in January 2007. The purpose of the project was to create a simulation that would stress the decision-making associated with a large bank failure, enhance the FDIC's ability to determine an effective resolution strategy, advance knowledge of the process, and identify lessons learned. A steering committee of FDIC executives is leading the project and Corporate University is directing it. A contractor was hired to design the simulation. During the reporting



Strategic Goal 5: FDIC Resources Management: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

period, the OIG continued to monitor the project. We need to be ready for any large failure and determine whether fraud is a contributing factor. We also need to be prepared to review the circumstances that cause a large bank failure and make recommendations, if appropriate, to strengthen the regulatory process.

FDIC Debtor Makes Restitution Payment of \$348,314

From an investigative standpoint, the OIG continues to conduct concealment of assets investigations to protect the FDIC's interests as receiver of a failed institution. Typically, in such cases, the OIG pursues instances where an individual commits a fraud to avoid paying the FDIC civil settlements, court-ordered restitution, and other payments as the institution receiver. During the reporting period, one such debtor made a substantial payment as a result of the OIG's preliminary investigative work.

Following the initiation of an OIG investigation and the issuance of grand jury subpoenas for records, an FDIC debtor who had claimed to be insolvent made a payment of \$348,314 toward his indebtedness. The debtor, who owes the FDIC a total of \$841,605, has been making monthly payments of several hundred dollars for 3 years and had claimed that his financial situation prevented him from paying anything more. The OIG and the Department of Justice are continuing to investigate the financial statements previously submitted by the debtor.

The FDIC manages and utilizes a number of critical strategic resources to carry out its mission successfully, particularly its financial, human, information technology (IT), and physical resources. The Corporation does not receive an annual appropriation, except for its OIG, but rather is funded by the premiums that banks and thrift institutions pay for deposit insurance coverage, the sale of assets recovered from failed banks and thrifts, and from earnings on investments in U.S. Treasury securities.

The Board approved a \$1.1 billion corporate operating budget for 2007, approximately 4.6 percent higher than for 2006. The approved budget provides funding for additional compliance examiners, increased employee training, enhanced IT security and privacy programs, and completion of systems changes required to support the implementation of deposit insurance reform. The Corporation's 2007 spending on multi-year investment projects separately approved by the Board is expected to be approximately \$19 million to \$23 million.

The Corporation is continuing to operate in the context of its New Financial Environment, intended to meet current and future financial

management and financial information needs; improve corporate financial business processes; and redirect resources from transaction processing to analysis, risk management, and decision support.

Financial resources are but one aspect of the FDIC's critical assets. The Corporation's human capital is also vital to its success. Because of the projected retirements of a large number of long-serving employees, the FDIC has made efforts to reshape its workforce with the implementation of the Corporate Employee Program, the Succession Management Program, and the Leadership Development Program. Throughout the reshaping of its workforce, the FDIC maintains its commitment to a working environment of high integrity and to the achievement of its mission.

Technological advances have produced tools that all workers today would be lost without. IT drives and supports the manner in which the public and private sector conduct their work. At the FDIC, the Corporation seeks to leverage IT to support its business goals in insurance, supervision and consumer protection, and receivership management, and to improve the operational efficiency of its business processes. The financial

services industry employs technology for similar purposes.

Along with the positive benefits that IT offers comes a certain degree of risk. In that regard, information security has been a long-standing and widely acknowledged concern among federal agencies. The E-Government Act of 2002 recognized the importance of information security. Title III of the E-Government Act, entitled FISMA, requires each agency to develop, document, and implement an agency-wide information security program to provide adequate security for the information and information systems that support the operations and assets of the agency. Section 522 of the Consolidated Appropriations Act of 2005 requires agencies to establish and implement comprehensive privacy and data protection procedures and have an independent third-party review performed of their privacy programs and practices.

Business continuity and disaster recovery are foremost concerns to all federal agencies. The FDIC must be sure that its emergency response plans provide for the safety and physical security of its human resources and ensure that its business continuity planning and disaster recovery capabilities keep critical business

functions operational during any emergencies, including threats to public health such as a pandemic influenza.

The Federal Deposit Insurance Act empowers the FDIC to enter into contracts to procure goods and services. Over the past several years, the Corporation has increased its reliance on outsourcing for services such as IT infrastructure support, IT application system development, and facilities maintenance. Also, a number of new contracting vehicles have been implemented. For example, the Corporation combined approximately 40 IT-related contracts into one contract with multiple vendors for a total program value of \$555 million over 10 years.

As an integral part of its stewardship of the insurance funds, the FDIC has established a risk management and internal control program. The Office of Enterprise Risk Management (OERM) is the corporate oversight manager for internal controls and risk management. OERM works with FDIC divisions and offices, helping them to identify, evaluate, monitor, and manage their risks.

To promote sound governance and effective stewardship of FDIC

strategic resources, the OIG's 2007 performance goals were as follows:

- Evaluate corporate efforts to fund operations efficiently, effectively, and economically.
- Assess corporate human capital strategic initiatives.
- Promote integrity in FDIC internal operations.
- Promote alignment of IT with the FDIC's business goals and objectives.
- Promote IT security measures that ensure the confidentiality, integrity, and availability of corporate information.
- Promote personnel and physical security.
- Evaluate corporate contracting efforts.
- Monitor corporate risk management and internal control efforts.

OIG Work in Support of Goal 5

The OIG committed a number of audit and evaluation resources to work in this strategic goal area during the reporting period. One of our most significant undertakings in this area was our work under FISMA, including an assessment of the FDIC's privacy

program activities and initiatives. Additionally, among other assignments, we performed an evaluation of the FDIC's use of performance measures and another evaluation of the Corporation's IT application services contracting process, as discussed below.

Federal Information Security Management Act Evaluation – 2007

We contracted with KPMG, LLP (KPMG) to conduct an independent evaluation of the FDIC's information security program and practices pursuant to FISMA. FISMA requires federal agencies, including the FDIC, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluation to the Office of Management and Budget.

Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding the sensitive information it collects and manages in its role as federal deposit insurer of banks and savings associations. Ensuring the integrity, availability, and confidentiality of this information in an environment of increasingly sophisti-

cated security threats requires a strong, enterprise-wide information security program.

KPMG reported that the FDIC has made significant progress in recent years in addressing the information security provisions of FISMA and the National Institute of Standards and Technology. This progress is noteworthy given the considerable increase in information-security-related requirements levied on federal agencies. KPMG found that the FDIC established policies and procedures in substantially all of the security control areas evaluated. In addition, KPMG noted particular strength in the areas of *Information Security Governance, Incident Response, and Awareness and Training* and that additional improvements were underway at the close of the evaluation.

These accomplishments are notable. However, KPMG identified a number of information security control deficiencies warranting management attention. Addressing these security control deficiencies will contribute to the FDIC's ongoing efforts to achieve reasonable assurance of adequate security over corporate information resources. KPMG's report identifies steps that the Corporation can take to strengthen security controls in

the priority areas of *Access Control; Identification and Authentication; Certification, Accreditation, and Security Assessments; Risk Assessment; Personnel Security; and Audit and Accountability*. In many cases, the FDIC was already working to improve security controls in these areas during KPMG's evaluation. We will follow up on the security control deficiencies identified in this report as part of future FISMA evaluations.

The FDIC's Privacy Program and Initiatives

In fulfilling its legislative mandate of insuring deposits, supervising financial institutions, and managing receiverships and in its role as a federal employer and acquirer of services, the FDIC creates and acquires a significant amount of personally identifiable information (PII) (e.g., name, Social Security number, or biometric records) related to depositors and borrowers at FDIC-insured financial institutions and FDIC employees and contractors. Much of the PII managed by the FDIC and its contractors falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure.

On July 25, 2007, the Office of Management and Budget (OMB)

issued Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The memorandum directs agency Inspectors General to provide relevant status information on agency privacy programs. In addition, the memorandum directs agency IGs to assess (1) the quality of their agencies' process for conducting privacy impact assessments (PIA) of systems containing PII and (2) the progress the agency is making in implementing PII safeguards recommended in OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 2, 2006. OMB defines a PIA as a process for (1) examining the risks of using IT to collect, maintain, and disseminate PII from or about members of the public and (2) identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

Consistent with the provisions of OMB Memorandum M-07-19, we conducted an audit to assess the status of the FDIC's privacy program activities and initiatives. Our work focused on the status of the FDIC's efforts to address selected key provisions of privacy-related memoranda recently issued by OMB.

We reported that the FDIC continues to take action to safeguard its PII and related systems and address privacy-related provisions of recent OMB memoranda. Of particular note, the FDIC has appointed a senior agency official for privacy, conducted privacy reviews prescribed by OMB, and provided employees and contractors with privacy-awareness training. Importantly, the FDIC has established a process for conducting PIAs of its information systems containing PII that is consistent with relevant privacy-related policy, guidance, and standards. In addition, the FDIC is making satisfactory progress in implementing the provisions of OMB Memorandum M-06-15. The FDIC is also working to complete a number of ongoing privacy program initiatives to safeguard its PII and related systems.

This report contains no recommendations. We plan to follow up on the status of the FDIC's ongoing privacy initiatives as part of future reviews.

IT Events Analysis

The Corporation's risk management program emphasizes guidance provided by the Treadway Commission's Committee of Sponsoring Organizations (COSO) for implementing individual division/

office risk management programs. The FDIC's Division of Information Technology (DIT) is in the early stage of adopting the Control Objectives for Information and Related Technology (COBIT®) framework, created by the IT Governance Institute, as part of the division's risk management program. The COBIT® framework links DIT's IT control program objectives to the risk management activities defined by COSO.

COBIT® organizes IT activities into business-oriented processes with control objectives to help organizations ensure that IT investments align with business goals and objectives and that IT-related risks and opportunities are appropriately managed.

One of our projects during the reporting period was to develop an events-based approach for planning and prioritizing audit coverage of the FDIC's IT program and operations. An event affects achievement of objectives and can have a negative impact, a positive impact, or both. Events with negative impact represent risks. Events with positive impact may offset negative impacts or represent opportunities.

Our events-based analysis is intended to provide increased assurance that

IT audit resources are used consistent with, and promote the achievement of, the FDIC's business goals and objectives. We received feedback on a draft of our project results from the FDIC's Chief Information Officer and DIT staff and incorporated those comments as appropriate.

IT Application Services Contracting

The FDIC fulfills its IT service requirements through the use of contracts with various vendors. To enhance the efficiency and effectiveness of procurement of IT services, the FDIC Board of Directors approved \$554.8 million to initiate a new Information Technology Application Services (ITAS) contracting process. The resulting ITAS approach commenced in 2005 and included the consolidation of existing IT contracts; the development of performance-based contracts; the establishment of long-term partnerships with a small pool of pre-qualified IT service vendors; and the issuance of IT service task orders to that vendor pool.

We conducted an evaluation to determine whether the ITAS process strikes the proper balance between timely issuance of task orders and the maintenance of proper risk controls.

To that end, we reviewed a sample selection of task orders to determine the current issuance process as well as to identify process controls. Further, we contracted with procurement process experts from CACI Dynamic Systems, Inc. (CACI) to both benchmark the FDIC task order issuance timeline against other federal agencies with similar procurement programs and to identify government and private sector best practices that may enhance the ITAS process.

We reported that the ITAS contracting approach contains appropriate controls over task order awards. In addition, the ITAS process generally provides for fair competition among the pool of four ITAS vendors. Further, the standard labor category hourly price rates required to be used by all four ITAS vendors and the price realism determinations enhance control over the price paid for each task order. However, we found that the efficiency of the ITAS task order process could be improved, as the time frames were generally longer than those for Federal Acquisition Regulations-based agencies using similar contracting vehicles.

We provided suggested actions to FDIC management to improve the ITAS contracting process but did not make formal recommendations. Additionally,

procurement experts from CACI briefed Division of Administration and DIT management concerning best practices used by other federal agencies for similar procurement programs. FDIC management indicated it had initiated, or planned to take, actions to address our suggestions.

Use of Performance Measures

Congress and OMB have worked to implement a statutory and management reform framework to improve the performance and accountability of the federal government. Congress enacted the Government Performance and Results Act of 1993 (GPRA) as a key element of this framework. GPRA seeks to improve the management of federal programs, as well as their effectiveness and efficiency, by establishing a system under which agencies set goals for program performance and measure their results.

The FDIC meets GPRA requirements through the issuance of a strategic plan, an annual performance plan (APP), and a performance and accountability report (PAR). The FDIC also has implemented additional performance measurement processes in the form of Corporate Performance Objectives and balanced scorecards,



Strategic Goal 6: OIG Internal Processes: Build and Sustain a High- Quality OIG Work Environment



While the OIG is focused on the FDIC's programs and operations, we have an inherent obligation to hold ourselves to the highest standards of performance and conduct. Like any organization, we have processes and procedures for conducting our work; communicating with our clients, staff, and stakeholders; managing our financial resources; aligning our human capital to our mission; strategically planning and measuring the outcomes of our work; maximizing the cost-effective use of technology; and ensuring our work products are timely, value-added, accurate, and complete and meet applicable professional standards.

To build and sustain a high-quality OIG work environment, the OIG's 2007 performance goals were as follows:

- Encourage individual growth through personal development;
- Strengthen human capital management and leadership development;
- Foster good client, stakeholder, and staff relationships;
- Ensure quality and efficiency of OIG audits, evaluations, investigations, and other operations;
- Enhance strategic and annual performance planning and performance measurement; and
- Invest in cost-effective and secure IT.

Encourage Individual Growth Through Personal Development

❖ Conducted a mid-year assessment of the OIG's pilot training and development plans for 2007 for auditors, evaluators, and investigators. The plans reflect a minimum requirement of 44 hours of training to be taken by auditors and program analysts in the Office of Audits (OA) and the Office of Evaluations (OE) and a minimum requirement of 64 hours of training for criminal investigators in the Office of Investigations (OI).

❖ Nominated and supported five members of the OIG to attend long-term graduate banking school programs sponsored by Stonier, the Southeastern School of Banking at Vanderbilt University, and the University of Wisconsin to enhance OIG staff expertise and knowledge of the banking industry.

❖ Carried out the OIG's mentoring program and made plans for continuing and enhancing the program in fiscal year 2008.

as well as other performance metrics related to individual contracts and system development efforts.

We conducted an evaluation during the reporting period to assess the performance measurement processes that the FDIC uses to monitor corporate performance. We determined that the FDIC has developed and implemented multiple performance measurement processes and approaches that serve various stakeholder needs and that FDIC managers use to varying levels to manage and monitor program performance. Collectively, we found that the FDIC uses performance measures to make management decisions to improve programs and results. We also observed that the FDIC employs practices to enhance the use of performance information.

The FDIC also communicates performance measures externally by publishing a strategic plan, APP, and PAR. These documents generally contain information required by GPRA and implementing guidance issued by OMB. Notwithstanding, we identified opportunities to enhance the APP and PAR to increase transparency, improve corporate accountability, and provide information to aid in congressional decision-making, all key purposes of the GPRA legislation.

We made three recommendations to strengthen the performance measurement processes. The FDIC did not concur with the recommendations, but has taken or proposed actions that meet the intent of two of the recommendations. The final recommendation addressed enhancements we determined were needed in the FDIC's GPRA program evaluation function. After considering management's response, we continue to believe that the FDIC would benefit from implementing our recommendation. Nevertheless, because GPRA does not specifically require agencies to conduct program evaluations, we accepted management's decision not to take action on this recommendation.

OIG Policy Reviews

During the reporting period, we reviewed 17 draft corporate policies and raised 7 policy issues for consideration in the draft documents related to: *Publishing FDIC Information via the Internet and FDICnet*, *Policy and Procedures for Memorandums of Understanding and Interagency Agreements*, *the FDIC's Enterprise Architecture Program*, and *the FDIC Records Management Program Manual*.

Our comments are incorporated in final policy, as determined by FDIC management.

Ongoing Audit and Evaluation Work

Ongoing work in this strategic goal area includes an audit of the Corporation's laptop computer replacement initiative. We are determining whether there are appropriate controls in place. We are also completing evaluations related to the FDIC's transit subsidy program, the corporate telework program, and contract rationalization. Finally, as of the end of the reporting period, we were in the process of finalizing our report on the FDIC's risk management program and also preparing a report on the FDIC's Claims Administration System.

Strengthen Human Capital Management and Leadership Development

❖ The 2007 pilot training and development plans for OIG staff include 8 hours of leadership training for each person. We disseminated information and guidance on existing leadership development programs to all OIG staff. We began to plan establishing an OIG Leadership Development Program, using the CU Leadership Development Program as a framework for incorporating unique OIG requirements.

❖ Implemented use of an end-of-assignment feedback form for OA and OE to help foster continuous performance dialogue among all OIG staff. Made plans to assess the success of the process and address any necessary modifications.

❖ Took a number of steps to update the OIG's business continuity and emergency preparedness plans, including updating emergency contact information; equipping shelter-in-place rooms in OIG office space in coordination with the Division of Administration and DIT; developing an OIG Emergency Response Plan Quick Reference Guide; and revamping the OIG Business Continuity Plan

to incorporate revised delegations of authority, business functions, and requirements for off-site storage of vital OIG records.

❖ Updated and provided OIG workforce data to OIG senior executives for their use in formulating strategic staffing plans for fiscal year 2008 and beyond.

Foster Good Client, Stakeholder, and Staff Relationships

❖ Maintained Congressional working relationships by providing our Semiannual Report to the Congress for the 6 month period ending March 31, 2007; providing information related to HR 2547, the FDIC Enforcement Enhancement Act; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; attending FDIC-related hearings on issues of concern to various oversight committees; informing the cognizant Subcommittees of the Senate and House Committees on Appropriations of our fiscal year 2007 appropriation baseline; and planning for Inspector General briefings and congressional staff participation at the OIG's Emerging Issues Symposium in November 2007.

❖ Communicated with the FDIC Chairman, Vice Chairman, Director

Curry, and other senior FDIC officials through the Inspector General's regularly scheduled meetings with them and through other forums.

❖ Participated in DSC regional meetings to provide general information regarding the OIG and OI case studies on bank frauds that are of importance to DSC and the banking industry.

❖ Held quarterly meetings with FDIC Directors and other senior officials to keep them apprised of ongoing audit and evaluation reviews and results.

❖ Kept DSC, DRR, the Legal Division, and other FDIC program offices informed of the status and results of our investigative work impacting their respective offices. This is accomplished by notifying FDIC program offices of recent actions in OIG cases and providing OI's quarterly reports to DSC, DRR, the Legal Division, and the Chairman's Office outlining activity and results in our cases involving closed and open banks, asset and debt cases.

❖ Participated at Audit Committee meetings and presented results of significant assignments for consideration by Committee members.

❖ Supported the President's Council on Integrity and Efficiency (PCIE) by attending monthly PCIE meetings

and participating in PCIE Audit and Inspection & Evaluation Committee meetings, attending the annual PCIE/ Executive Council on Integrity and Efficiency conference, hosting a joint PCIE/Executive Council on Integrity and Efficiency meeting, hosting a 2-week session of Introductory Auditor Training at the FDIC's Virginia Square training site, providing support to investigative meetings and training, and volunteering to produce the fiscal year 2007 Progress Report to the President.

❖ Met with representatives of the OIGs of the financial regulatory agencies (Board of Governors of the Federal Reserve System, Department of the Treasury, National Credit Union Administration, Securities and Exchange Commission, Farm Credit Administration, Commodity Futures Trading Commission, Federal Housing Finance Board) to discuss audit and investigative matters of mutual interest.

❖ Continued to hold quarterly meetings of the OIG's Employee Advisory Group. The new Employee Advisory Group is comprised of three employees from OI, two employees from OA, and one employee each from OE and the Office of Management, all of whom meet with the Inspector General to discuss issues of OIG-wide interest or concern.

❖ Continued to post and/or update information on the FDIC OIG internet (www.fdicig.gov) and intranet sites to ensure transparency and accessibility to OIG products, including Semiannual Reports to the Congress, audit and evaluation reports, and investigation-related press releases.

Ensure Quality and Efficiency of OIG Audits, Evaluations, Investigations, and Other Operations

❖ Continued revising OA's Policy and Procedures Manual to address changes in the performance audit standards and process changes deemed advisable as a result of an internal assignment management review and the external peer review results.

❖ Trained OA and OE staff on the Government Accountability Office 2007 revision of Government Auditing Standards as part of an OIG-wide conference in April 2007. The new standards will be effective for engagements beginning on or after January 1, 2008.

❖ Received an unmodified opinion from the Department of State OIG as a result of its peer review of our audit operations.

❖ Completed internal reviews of OI's Western Regional Offices (Dallas and Chicago) and reported no instances of noncompliance with OI policies and procedures.

❖ Worked with members of the FDIC's Acquisition Services Branch to award a contract to a qualified firm to provide audit and evaluation services to the OIG to enhance the quality of our work and the breadth of our expertise as we conduct audits and evaluations.

❖ Continued to maintain a project management tracking and reporting process for internal OIG projects. The milestone documents for projects were updated regularly and used to track the status and progress of the OIG's internal improvement projects.

Enhance Strategic and Annual Planning and Performance Measurement

❖ Continued efforts to conduct the OIG's fiscal year 2008 business planning process, including review of the fiscal year 2007 planning process to determine what worked well and what could be improved, internal OIG meetings to validate strategic and performance goals, outreach meetings to FDIC Divisions and Offices, and research and analysis of significant

activities within the Corporation and the financial services industry.

❖ Held an OIG conference in April 2007 to emphasize and explain the OIG's strategic business planning and goals and the measures to assess OIG performance in carrying out the plan.

❖ Monitored OIG progress in meeting fiscal year 2007 strategic and performance goals through use of the OIG Dashboard and regularly scheduled status meetings with OIG executives.

Invest in Cost-Effective and Secure IT

❖ Integrated planning for OIG IT needs in the annual business planning process by developing specific IT-related initiatives as key efforts to be monitored on a continuous basis.

❖ Coordinated extensively with DIT to migrate the OIG's systems and files to the OIG's new servers.

❖ Collaborated with DIT to replace OIG laptops and successfully completed all installations in headquarters and field office sites.

❖ Continued to partner with DIT to ensure the security of OIG information in the FDIC computer network infrastructure.

❖ Attended a May 2007 FDIC-sponsored Gartner Group presentation on emerging technologies for business intelligence and data warehousing applications.

❖ Attended several meetings of the FDIC's Enterprise Architecture Board.

❖ Took steps to identify and explore options and requirements to streamline, enhance, and improve the collection and reporting of information needed to manage OIG audits and evaluations. Held multiple meetings between the OIG's TeamMate Update project team and DIT to plan for, test, and install the latest update of TeamMate by December 2007.

❖ Continued efforts to improve the OIG's Training System and the process of requesting and approving training for OIG professional, supervisory, and administrative staff using the system.

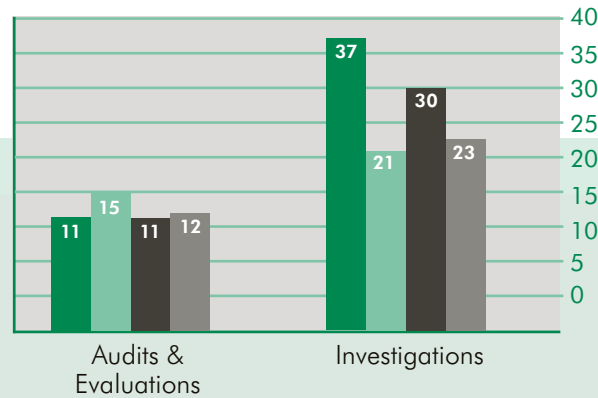
Cumulative Results (2-year period)

Nonmonetary Recommendations	
October 2005 - March 2006	34
April 2006 - September 2006	48
October 2006 - March 2007	35
April 2007 - September 2007	7

Products Issued and Investigations Closed

LEGEND

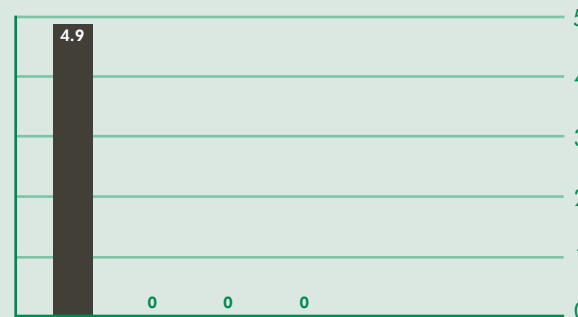
- Oct 05 - Mar 06
- Apr 06 - Sept 06
- Oct 06 - Mar 07
- Apr 07 - Sept 07



Questioned Costs/Funds Put to Better Use (in millions)

LEGEND

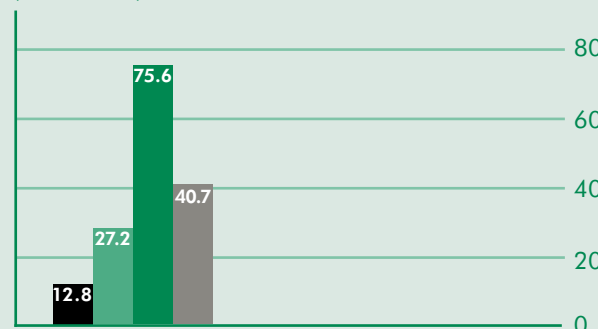
- Oct 05 - Mar 06
- Apr 06 - Sept 06
- Oct 06 - Mar 07
- Apr 07 - Sept 07



Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations (in millions)

LEGEND

- Oct 05 - Mar 06
- Apr 06 - Sept 06
- Oct 06 - Mar 07
- Apr 07 - Sept 07



Fiscal Year 2007 Performance Report

This performance report presents an overview of our performance compared to our fiscal year 2007 annual performance goals in our Business Plan. It provides a statistical summary of our qualitative goals as well as a narrative summary of performance results by Strategic Goal. It also shows our results in meeting a set of quantitative goals that we established for the year. Our complete 2007 Business Plan is available at www.fdicig.gov

We formulated six strategic goals, as shown in the table below. Each of our strategic goals, which are long-term efforts, has annual performance goals and key efforts that represent our initiatives in fiscal year 2007 toward accomplishing the strategic goal. The table reflects the number of performance goals that were Met, Substantially Met, or Not Met. This determination was made through ongoing discussions at the OIG Executive level and a qualitative assessment as to the impact and value of the audit, evaluation, investigation, and other work of the OIG supporting these goals throughout the year.

As shown in the table, we met or substantially met all of our performance goals in fiscal year 2007. A discussion of our success in each of the goals follows the table.

Fiscal Year 2007 Annual Performance Goal Accomplishment (Number of Goals)				
Strategic Goals	Performance Goals			
	Met	Substantially Met	Not Met	Total
Supervision: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly	1	1		2
Insurance: Help the FDIC Maintain the Viability of the Insurance Fund	1			1
Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy	2	1		3
Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships	2			2
FDIC Resources Management: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources	6	2		8
OIG Internal Processes: Build and Sustain a High-Quality OIG Work Environment	6			6
Total	18	4		22
Percentage	82	18		100

Goal 1: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly

Our work in helping to ensure that the nation's banks operate safely and soundly takes the form of audits, investigations, evaluations, and extensive communication and coordination with FDIC divisions and offices, law enforcement agencies,

other financial regulatory OIGs, and banking industry officials. During fiscal year 2007, in audit reports issued, we made recommendations to enhance protection from risks associated with e-banking, ensure that examinations adequately consider the reliability of appraisals and sufficiency of insurance coverage when evaluating an institution's lending activities, and strengthen the supervisory approach

for ensuring financial institution compliance with Office of Foreign Assets Control compliance programs. We continued work on the FDIC's evaluation of institution compliance with the anti-money laundering and terrorist financing provisions of the USA PATRIOT Act. We also audited examination procedures for assessing controls to protect customer and consumer information at multi-regional data processing servicers.

With respect to investigative work, as a result of cooperative efforts with U.S. Attorneys throughout the country, numerous individuals were prosecuted for financial institution fraud, and we achieved successful results in combating a number of emerging mortgage fraud schemes during the fiscal year. Particularly noteworthy results include a restitution order in the aggregate amount of \$31.7 million that was issued in connection with our investigation of Hamilton Bank and bank fraud on the part of former bank officers. The restitution was ordered on the former chairman of the board and chief executive officer, and his codefendants, the former president and the former chief financial officer of the failed bank. In another significant case, in the U.S. District Court for the District of Colorado, the former BestBank

owner and chief executive officer and chairman of the board of directors, the former president and director, and the former chief financial officer were found guilty of 15 felony counts of fraud and conspiracy related to BestBank's \$248 million failure in 1998. The former president and director and the former chief financial officer were sentenced to 90 months of incarceration, to be followed by 3 years of supervised release and 72 months of incarceration, to be followed by 3 years of supervised release, respectively. The judge did not order restitution but ordered forfeitures of \$4.7 million for the former president and director and more than \$92,000 for the former chief financial officer.

As for mortgage frauds, particularly noteworthy results include the stiff sentencing of the former senior vice president of mortgage operations at nBank and two mortgage brokers for defrauding the bank of nearly \$11 million. In another case, a defendant was convicted in an \$11 million mortgage loan fraud in New York. Another of our investigations led to the convictions of a former Wall Street executive and a co-conspirator in a \$12 million securities fraud conspiracy. These individuals were ordered to pay back nearly all of that amount in restitution to the government.

Goal 2: Help the FDIC Maintain the Viability of the Insurance Fund

Audit work related to the FDIC's dedicated examiner program confirmed that the Corporation's Dedicated Examiner Program is contributing to the FDIC's efforts to assess and quantify the risks posed by large institutions to the Deposit Insurance Fund. Given that the FDIC is not generally the primary federal regulator for the largest financial institutions, this program has placed dedicated examiners in the six largest insured depository institutions to work in cooperation with primary supervisors and bank personnel to obtain real-time access to information about the risk and trends in those institutions. Similarly, we reported positive results related to the Shared National Credit program, an interagency program to provide periodic credit risk assessment of large, complex credits held or agented by supervised institutions.

We would also note that all of the OIG's investigative results described in support of Goal 1 above also support the Corporation in its efforts to maintain the viability of the insurance fund.

Goal 3: Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy

Audits and investigations contributed to the FDIC's protection of consumers in several ways. We issued a report on information technology (IT) examination coverage of financial institutions' oversight of technology service providers and made recommendations to help in protecting customers from identity theft and institutions from fraud and reputational and other risks associated with unauthorized access to or use of customer information. As a result of audit work related to amendments to Community Reinvestment Act regulations, we suggested strengthened examiner guidance for implementing and reporting on community development tests and development of a strategy for measuring the impact of amendments to the regulations. We issued a report on the FDIC's assessment of institutions' compliance management systems, reporting that FDIC examiners had adequately assessed the key components of institution compliance management systems—the board of directors and management oversight, the compliance program, and periodic compliance audits.

From an investigative standpoint, our Electronic Crimes Unit (ECU) responded to phishing schemes where the FDIC and OIG Websites were misused to entice consumers to divulge personal information and successfully shut down several Web sites used for such purposes. The ECU was also successful in deactivating Web sites and/or fax numbers involving fraudulent claims of FDIC insurance or affiliation. In that connection, we also continued to monitor the progress of H.R. 2547, The FDIC Enforcement Enhancement Act, a bill to amend the Federal Deposit Insurance Act to prevent misrepresentation about deposit insurance coverage, and for other purposes.

Goal 4: Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

We completed an assignment to evaluate the design and implementation of selected controls established by the Division of Resolutions and Receiverships to safeguard sensitive information collected and maintained in electronic form in resolution and receivership activities at FDIC-insured institutions. We made four recommendations to address vulnerabilities, and the Corporation took prompt action

in response. We also continued to monitor the FDIC's Strategic Readiness Project to gain a better understanding of the implications of a large bank failure and corresponding resolution scenario and offered OIG perspectives in the interest of ensuring the success of that corporate initiative.

We also continued to pursue concealment of assets investigations related to the more than \$1.7 billion in criminal restitution that the FDIC is owed. In connection with one such case worked in conjunction with the FDIC Legal Division, the former chief executive officer of Sunbelt Savings and Loan, Dallas, Texas, was sentenced to 97 months of incarceration and ordered to pay a criminal forfeiture of more than \$2 million to the U.S. government and restitution of more than \$300,000 to the FDIC.

Goal 5: FDIC Resources Management: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

We issued a number of audit and evaluation reports in this goal area and made recommendations to strengthen contract planning and management for business continuity,

ensure appropriate use of information in an identifiable form and enhanced protection of sensitive FDIC data, strengthen contract administration and oversight of IT support services for the Corporation, and improve information security controls. We also made suggestions to improve the IT application services contracting process and recommendations to enhance the FDIC's performance measurement processes.

We issued the results of our review of a comprehensive review of the FDIC's information security program and practices, in accordance with the Federal Information Security Management Act (FISMA). Our 2007 report notes strength in the areas of information security governance, incident response, and awareness training. It also identifies steps the Corporation can take to strengthen security controls in the priority areas of access control; identification and authentication; certification, accreditation, and security assessments; risk assessment; personnel security; and audit and accountability. In a related FISMA product, we reported that the FDIC continues to take action to safeguard its personally identifiable information and related systems. We also promoted integrity in FDIC

internal operations through ongoing OIG Hotline referrals, investigations of employee cases, and coordination with the FDIC's Ethics Office.

Goal 6: OIG Internal Processes: Build and Sustain a High-Quality OIG Work Environment

We focused increased attention on a number of activities in this goal area throughout the fiscal year. We held an OIG-wide conference, the theme of which was *Change, Challenge, Choices* to engage all OIG employees in the strategic and performance goals and efforts of the OIG. As part of that conference, Office of Audits and Office of Evaluations staff received training on the 2007 revisions to the Government Auditing Standards, and our investigative staff received their required Legal Update training. We encouraged individual growth through professional development by way of initiatives such as training and development and career development plans for OIG staff, expanding the OIG mentoring program, and offering opportunities for OIG staff to attend graduate schools of banking. We strengthened human capital management and leadership development by developing and implementing end-of-assignment feedback mechanisms for staff, and incorporating leadership training in training

and development plans. To ensure the safety and security of OIG staff, resources, and operations, we updated and strengthened the OIG's business continuity and emergency preparedness plans and procedures.

Our office continued to foster positive stakeholder relationships by way of OIG Executives' meetings with FDIC Executives; presentations at Audit Committee meetings; Congressional interaction; coordination with financial regulatory OIGs, other members of the Inspector General community, other law enforcement officials, and the Government Accountability Office. New members of the OIG employee Advisory Group took office and met regularly throughout the year. We also maintained and updated the OIG Web site to provide easily accessible information to stakeholders interested in our office and the results of our work.

Our Office of Audits conducted internal quality control reviews and underwent a peer review conducted by the Department of State OIG, and our Office of Investigations conducted internal quality control reviews of the Chicago and Dallas Office investigative operations. Office of Audits began work to revise audit policies and procedures to address changes

in the 2007 revision to *Government Auditing Standards*, process changes resulting from an internal assignment management review, and external peer review results. To ensure cost-effective and secure IT, we continued to coordinate closely with the FDIC's Division of Information Technology. We also completed a laptop replacement project in OIG headquarters and field offices. We took steps to identify and evaluate options to streamline, enhance, and improve collection and reporting of information to manage OIG audits and evaluations. We implemented upgrades to the OIG's training system and updated the OIG's internal Business Plan 2007 Dashboard to capture progress on achievement of strategic and performance goals.

With respect to planning and performance measurement, in formulating our Business Plan for 2008, we conducted a series of meetings to ensure appropriate audit and evaluation coverage and investigative activity to address the risks at the FDIC and in the financial services industry. These included outreach sessions and other meetings with many FDIC Divisions and Office representatives. We also focused on carefully tracking costs and integrating budget considerations in our planning activities.

Quantitative Performance Summary - Fiscal Year 2007

Performance Measure	FY 2007 Target	FY 2007 Actual	Status
Financial Benefit Return ¹	100%	454%	Met
Other Benefits ²	100	131	Met
Past Recommendations Implemented ³	95%	96%	Met
Audit/Evaluation Reports Issued	26	23	Substantially Met
Audit/Evaluation Assignments Completed Within 30 Days of Established Milestones	90%	50%	Not Met
Investigation Actions ⁴	120	216	Met
Closed Investigations Resulting in Reports to Management, Convictions, Civil Actions, or Administrative Actions	80%	78%	Substantially Met
Investigations Accepted for Prosecution Resulting in Convictions, Pleas, and/or Settlements	70%	66%	Substantially Met
Investigations Referred for Prosecution or Closed Within 6 Months of Opening Case	85%	93%	Met
Closing Reports Issued to Management Within 30 Days of Completion of All Judicial Actions	100%	92%	Substantially Met

¹ Includes all financial benefits, including audit-related questioned costs; recommendations for better use of funds; and investigative fines, restitution, settlements, and other monetary recoveries divided by OIG's total fiscal year budget obligations.

² Benefits to the FDIC that cannot be estimated in dollar terms which result in improved services; statutes, regulations, or policies; or business operations and occurring as a result of work that the OIG has completed over the past several years. Includes outcomes from implementation of OIG audit/evaluation recommendations.

³ Fiscal year 2005 recommendations implemented by fiscal year-end 2007.

⁴ Indictments, convictions, informations, arrests, pre-trial diversions, criminal non-monetary sentencings, monetary actions, employee actions, and other administrative actions.

As noted in the table above, we did not meet our timeliness goal for audit and evaluation completion. We intend to devote increased attention to that goal area during fiscal year 2008.

Reporting Requirements

Information Required by the Inspector General Act of 1978, as amended

Index of Reporting Requirements - Inspector General Act of 1978, as amended

Reporting Requirements	Page
Section 4(a)(2): Review of legislation and regulations	65
Section 5(a)(1): Significant problems, abuses, and deficiencies.....	11-50
Section 5(a)(2): Recommendations with respect to significant problems, abuses, and deficiencies	11-50
Section 5(a)(3): Recommendations described in previous semiannual reports on which corrective action has not been completed.....	66-67
Section 5(a)(4): Matters referred to prosecutive authorities	10
Section 5(a)(5) and 6(b)(2): Summary of instances where requested information was refused	70
Section 5(a)(6): Listing of audit reports.....	68
Section 5(a)(7): Summary of particularly significant reports.....	11-50
Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs	69
Section 5(a)(9): Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use	70
Section 5(a)(10): Audit recommendations more than 6 months old for which no management decision has been made	70
Section 5(a)(11): Significant revised management decisions during the current reporting period	70
Section 5(a)(12): Significant management decisions with which the OIG disagreed.....	70

Review of Legislation and Regulations

The FDIC OIG is tasked under the Inspector General Act of 1978 with reviewing existing and proposed legislation and regulations relating to programs and operations of the Corporation and making recommendations in the semiannual reports required by section 5(a) concerning the impact of such legislation or regulations on the economy and efficiency in the administration of programs and operations administered or financed by the Corporation or the prevention and detection of fraud and abuse in its programs and operations. The Office of Counsel has been following the status of various bills relating to the Inspector General Community, particularly bills that would require some or all Inspectors General to perform audits regarding particular areas of agency operations, as well as a bill passed by the House of Representatives, forwarded to the Senate and referred to the Senate Banking Committee that would give the FDIC significant new enforcement authority with regard to misuses of the FDIC's name and logo. We are also monitoring bills related to the Freedom of Information Act. However, we have not provided written comments on those bills to Congress. The Office of Counsel reviewed and provided comments on draft FDIC directives related to FDIC Procedures for Processing Section 515 Requests for Information Correction, Records Management, Data Stewardship Program, Digital Library, Suitability of Contractors, and Ethics.

Table I: Significant Recommendations From Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

This table shows the corrective actions management has agreed to implement but has not completed, along with associated monetary amounts. In some cases, these corrective actions are different from the initial recommendations made in the audit reports. However, the OIG has agreed that the planned actions meet the intent of the initial recommendations. The information in this table is based on (1) information supplied by FDIC's Office of Enterprise Risk Management (OERM) and (2) the OIG's determination of closed recommendations for reports issued after March 31, 2002. These 15 recommendations from 11 reports involve improvements in operations and programs. OERM has categorized the status of these recommendations as follows:

Management Action in Process: (15 recommendations from 11 reports)

Management is in the process of implementing the corrective action plan, which may include modifications to policies, procedures, systems, or controls; issues involving monetary collection; and settlement negotiations in process.

Table I: Significant Recommendations From Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

Report Number, Title & Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action In Process		
05-016 Security Controls Over the FDIC's Electronic Mail (E-Mail) Infrastructure March 31, 2005	1 ♦	Ensure that division and office directors provide FDIC employees and contractors with sufficiently detailed guidance to facilitate informed decisions on when to encrypt sensitive e-mail communications.
EVAL-06-005 FDIC Safeguards Over Personal Employee Information January 6, 2006	1 ■	Develop and issue an overarching privacy policy for safeguarding personal employee information.
	15 ■	Revise FDIC Circular 1360.17, Information Technology Security Guidance for FDIC Procurements/Third Party Products to include security expectations and encryption requirements for contractors and vendors.
EVAL-06-014 FDIC's Industrial Loan Company Deposit Insurance Application Process July 20, 2006	5	Issue guidance clarifying corporate expectations for deposit insurance investigations and emphasizing that examiners should document the basis for their conclusions in the ROI.
06-023 Examiner Use of Home Mortgage Disclosure Act (HMDA) Data to Identify Potential Discrimination September 28, 2006	1 ■	Revise the Compliance Examination Manual guidance to specify when and how errors and omissions of current year HMDA data should be reported in compliance examination reports.
	2 ■	Provide additional examination guidance on how to determine and document third-party residential mortgage lending relationships for HMDA-reporting purposes.
06-024 Division of Supervision and Consumer Protection's Supervisory Actions Taken for Compliance Violations September 29, 2006	1 ■	Strengthen guidance related to the monitoring and follow-up processes for compliance violations.
06-025 Controls for Monitoring Access to Sensitive Information Processed by FDIC Applications September 29, 2006	3 ♦	Develop a written plan that defines a risk-based, enterprise-wide approach to audit logging and monitoring for the FDIC's portfolio of information systems.

♦ The OIG has received some information but has requested additional information to evaluate management's actions in response to the recommendation.

■ The OIG has not yet evaluated management's actions in response to the OIG recommendation.

Table I: Significant Recommendations From Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed (cont.)

Report Number, Title & Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
EVAL-06-026 FDIC's Contract Administration September 29, 2006	3	Establish firm target dates and devote dedicated resources for completing the Acquisition Policy Manual and related contracting documents, contract clauses, and provisions.
	13	Define requirements for the new automated procurement system, including to address the New Financial Environment shortcomings identified in this report.
07-003 FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005 January 10, 2007	1	Enhance the FDIC's privacy program by integrating key ongoing and planned program activities into a formally documented plan.
07-004 Interagency Agreement With the General Services Administration for the Infrastructure Services Contract January 10, 2007	2 ■	Strengthen the oversight process for proposed contract modifications involving significant reallocation of contract funding.
07-005 Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers (TSPs) February 5, 2007	1 ■	Revise the Information Technology-Risk Management Program guidance to ensure that examiners adequately assess financial institution compliance with the Interagency Guidelines provision pertaining to the oversight of TSPs.
07-008 FDIC's Implementation of the 2005 Amendments to the Community Reinvestment Act (CRA) Regulations March 30, 2007	1	Enhance examiner guidance to ensure examiners provide complete support in the performance evaluation reports for their conclusions for the community development test.
	3 ■	Develop a strategy for measuring CRA activities as a result of the amendments made to the regulations.

♦ The OIG has received some information but has requested additional information to evaluate management's actions in response to the recommendation.

■ The OIG has not yet evaluated management's actions in response to the OIG recommendation.

Table II: Audit Reports Issued by Subject Area

Audit Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title	Total	Unsupported	
Insurance				
AUD-07-011 September 13, 2007	FDIC's Dedicated Examiner Program for Large Insured Depository Institutions			
AUD-07-012 September 13, 2007	FDIC's Participation in the Shared National Credit Program			
Consumer Protection				
AUD-07-015 September 26, 2007	DSC's Examination Assessment of Financial Institutions' Compliance Management Systems			
Receivership Management				
AUD-07-010 September 5, 2007	Division of Resolutions and Receiverships Protection of Electronic Records			
Resources Management				
AP-07-001 May 11, 2007	Information Technology Events Analysis			
AUD-07-013 September 26, 2007	Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management			
AUD-07-014 September 27, 2007	Independent Evaluation of the FDIC's Information Security Program - 2007			
Totals for the Period		\$0	\$0	\$0

Table III: Evaluation Reports and Memoranda Issued

Number and Date	Title
Evaluation Reports	
EVAL-07-002 May 2, 2007	FDIC's Use of Performance Measures
EVAL-07-003 May 30, 2007	Information Technology Application Services Contracting Process
Evaluation Memoranda	
EM-07-002 May 8, 2007	Classifying Salary Costs in the New Financial Environment and Implementing Cost Management Reporting
EM-07-003 May 30, 2007	Follow-up Work Related to the FDIC's Contract Assessment Work
EM-07-004 August 16, 2007	Risk Designation Levels for Information Technology Staff and Privacy Act Contract Clauses in FDIC Contracts

Table IV: Audit Reports Issued with Questioned Costs

	Number	Questioned Costs	
		Total	Unsupported
A. For which no management decision has been made by the commencement of the reporting period.	0	0	0
B. Which were issued during the reporting period.	0	0	0
Subtotals of A & B	0	0	0
C. For which a management decision was made during the reporting period.	0	0	0
(i) dollar value of disallowed costs.	0	0	0
(ii) dollar value of costs not disallowed.	0	0	0
D. For which no management decision has been made by the end of the reporting period.	0	0	0
Reports for which no management decision was made within 6 months of issuance.	0	0	0

Farewells

Table V: Audit Reports Issued with Recommendations for Better Use of Funds

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period.	0	0
B. Which were issued during the reporting period.	0	0
Subtotals of A & B	0	0
C. For which a management decision was made during the reporting period.	0	0
(i) dollar value of recommendations that were agreed to by management.	0	0
- based on proposed management action.	0	0
- based on proposed legislative action.	0	0
(ii) dollar value of recommendations that were not agreed to by management.	0	0
D. For which no management decision has been made by the end of the reporting period.	0	0
Reports for which no management decision was made within 6 months of issuance.	0	0

Table VI: Status of OIG Recommendations Without Management Decisions

During this reporting period, there were no recommendations more than 6 months old without management decisions.

Table VII: Significant Revised Management Decisions

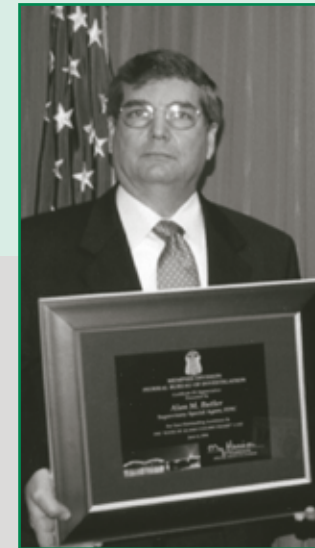
During this reporting period, there were no significant revised management decisions.

Table VIII: Significant Management Decisions with Which the OIG Disagreed

During this reporting period, there were no significant management decisions with which the OIG disagreed.

Table IX: Instances Where Information Was Refused

During this reporting period, there were no instances where information was refused.



Alan Butler

Alan Butler retired after 33 years of federal service. His career began in 1974 as an accountant with the Department of Housing and Urban Development then progressed to service as an auditor in the FDIC's Office of Corporate Audits and Internal Investigations in 1985. Later he was promoted to a senior auditor position, and in 1991, he was reassigned as a criminal investigator and promoted to a senior criminal investigator in the FDIC Office of Investigations, a position he held with distinction for nearly 16 years.

Throughout the years, he played a key role in carrying out the OIG mission at the FDIC. His versatile background served him well in his efforts to promote economy, efficiency, effectiveness, and integrity in a number of FDIC programs and operations.

Alan's work involving the Bank of Alamo, Alamo, TN is a prime example of his success. He worked tirelessly over the past several years on this case involving a highly complex bank fraud perpetrated by a group of individuals in rural Tennessee. A former Director and Chairman of the Board and the President and Chief Executive Officer of the Bank were indicted along with four bank customers on charges of conspiracy, money laundering, and bank fraud. Several of the defendants entered guilty pleas, and Alan's efforts were instrumental in the results of this case.



John English

John English retired in October 2007, after a federal career that began in April 1984 as an Audit Specialist with the U.S. Department of Agriculture, then progressed to service for the Resolution Trust Corporation, and finally, the FDIC. His career included work in a number of critically important areas, such as Financial Management Programs, Automated Data Processing Operations, Legal Services, and Information Technology Security and Privacy Program Operations. Since 1995, when he was assigned to the FDIC's OIG in Chicago, he worked on a number of progressively more difficult assignments.

During all of his assignments, he formed exceptional working relationships with agency officials and was genuinely respected by his colleagues. Of special note, his leadership, diligence, and innovation as the Auditor-in-Charge in planning, conducting, and reporting on the FDIC's information security program and practices greatly improved the security and effectiveness of the Corporation's business operations. His hard work and dedication to the success of all of the assignments he led will have a long-term, positive impact on the future operations of the Corporation.

Pictured left to right: Brian Smith, Special Agent, FBI; John Lucas, Special Agent FDIC OIG; Virginia Wright, Special Agent, FBI; Steve Hall, Financial Crimes Specialist, FDIC DRR

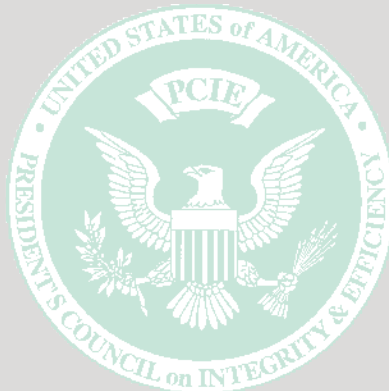


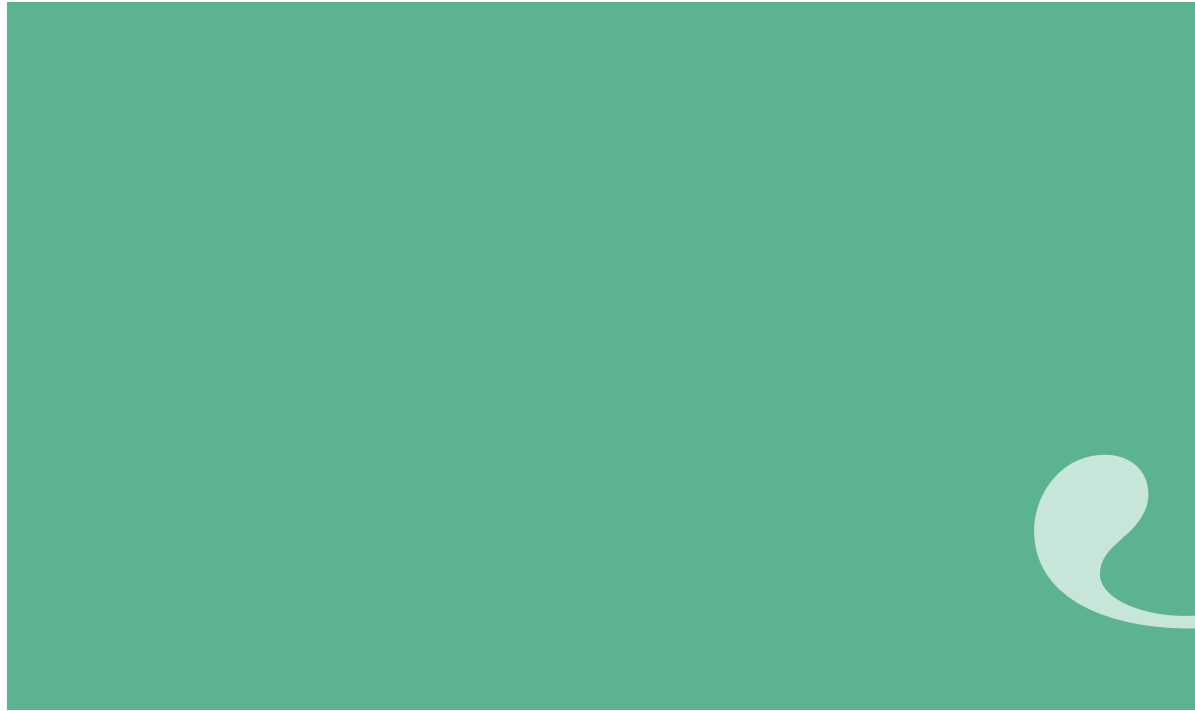
Congratulations

The OIG congratulates Special Agents John Lucas and Patrick Collins, who received an award for excellence from the President's Council on Integrity and Efficiency in October 2007. John and Patrick, along with Financial Crimes Specialist Steven Hall, one of our FDIC colleagues from the Division of Resolutions and Receiverships in Dallas, were members of a team whose outstanding efforts culminated in the prosecution of three individuals whose fraud scheme resulted in the failure of Universal Federal Savings Bank (Universal), Chicago, Illinois. All three subjects in the investigation pleaded guilty, received stiff fines, and made restitution to the FDIC and others for their criminal activity. The successful results of this white-collar crime case came about because of the dedication of a number of individuals from different agencies determined to work together to protect the integrity of the nation's banking system.

Joining John, Patrick, and Steven, were the other members of the Universal investigative/prosecution team:

- Brian Smith, Special Agent, FBI, Chicago, Illinois
- Edward G. Kohler, Assistant United States Attorney, Northern District of Illinois
- Robert W. Kent, Assistant United States Attorney, Northern District of Illinois
- Virginia H. Wright, Special Agent, FBI, Chicago, Illinois





The Office of Inspector General (OIG) Hotline is a convenient mechanism employees, contractors, and others can use to report instances of suspected fraud, waste, abuse, and mismanagement within the FDIC and its contractor operations. The OIG maintains a toll-free, nationwide Hotline (1-800-964-FDIC), electronic mail address (IGHotline@FDIC.gov), and postal mailing address. The Hotline is designed to make it easy for employees and contractors to join with the OIG in its efforts to prevent fraud, waste, abuse, and mismanagement that could threaten the success of FDIC programs or operations.

To learn more about the FDIC OIG and for complete copies of audit and evaluation reports discussed in this Semiannual Report, visit our Web site: <http://www.fdicig.gov>

To learn more about the FDIC OIG and for complete copies of audit and evaluation reports discussed in this Semiannual Report, visit our Web site: <http://www.fdicig.gov>

Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Drive
Arlington, VA 22226