I am pleased to present this 2020 issue of Interest magazine, highlighting the work of our special agents—those on the front lines of our fight against fraud, waste, and abuse in the programs and operations of the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection.

In this issue you will read about the important recent work of our special agents to bring wrongdoers to justice. You will also learn how the Office of Investigations is structured and the kinds of cases our special agents investigate. Special to this edition are feature articles describing how we cooperate with other law enforcement partners to solve financial crime cases and the rigorous training that special agents complete to prepare them for the complex array of cases they handle. I would like to thank our Office of Investigations for its hard work and dedication to combating fraud, waste, and abuse related to the Board and the Bureau.

About Inspector General Bialek:

Mark Bialek was appointed inspector general for the Board and the Bureau on July 25, 2011.

He has more than 39 years of experience in the inspector general community, including serving as the deputy inspector general for the U.S. Environmental Protection Agency, counsel to the inspector general at the U.S. Environmental Protection Agency, deputy counsel to the inspector general for the U.S. Department of State, associate counsel to the inspector general for the U.S. Department of Commerce, and chairman of the Council of Counsels to the Inspectors General.
Message From the Associate Inspector General for Investigations

The women and men of our Office of Investigations work tirelessly to root out wrongdoing against the Board; the Bureau; and by extension, the American people. I am proud to have worked alongside our special agents and staff for many years. As the associate inspector general for investigations, I am humbled to lead this group of dedicated individuals and eager to tackle the tasks ahead.

Our office continues to focus on ensuring that Board and Bureau programs and operations are free of fraud, waste, and abuse. This issue of Interest highlights the diversity of that work, from bringing down a bank general counsel’s over $56 million fraud scheme to uncovering another bank’s conspiracy to violate the Trading with the Enemy Act and the Cuban Asset Control Regulations.

We’re also ramping up outreach to the greater law enforcement community. Together with other federal agents, U.S. attorneys, and local law enforcement, we’re working to fight fraud, waste, and abuse related to Board and Bureau programs.

Enjoy this inside look at our operations.

About Associate Inspector General for Investigations Maye:

Leading the Office of Investigations, Gerald Maye oversees criminal, civil, and administrative investigations related to the programs and operations of the Board and the Bureau. Mr. Maye is a computer recovery specialist with 20 years of experience in federal law enforcement, much of it managing investigative operations, electronic crimes units, and the Office of Inspector General Hotline. He was previously a special agent in charge at the Social Security Administration OIG. Mr. Maye is an active leader on computer forensics in the inspector general community, having spoken at regional and national conferences, and he served as an adjunct professor at Stevenson University.
## Contents

**Office of Investigations** 5
- Field Offices
- Headquarters
- Types of Cases
- Process of Investigation
- Our Investigative Accomplishments

**Case Highlights** 9

**Special Report** 14
- Wells Fargo Agrees to Pay $3 Billion for Years-Long Fraud Exploiting Its Customers

**Feature Articles** 16
- Teaming Up With Other Agencies to Solve Financial Crime Cases
- Training for OIG Special Agents

**More About the OIG** 22

**OIG Hotline** 23
Office of Investigations

Our investigative team includes about 30 federal agents, forensic analysts, technical specialists, and support staff with a broad range of experience. Our agents are law enforcement officers with authority granted by the U.S. attorney general to carry firearms, make arrests, and execute warrants for search and seizure.

We routinely partner with other federal law enforcement agencies, the U.S. Attorney’s Offices throughout the country, and state and local law enforcement, adding value to complex investigations by virtue of our specialized knowledge and experience.

Field Offices

We have field offices in Chicago (Midwestern Region), Miami (Southeast Region), New York City (Northeast Region), and San Francisco (Western Region).

The field offices partner with the Federal Bureau of Investigation (FBI), the U.S. Secret Service, the Internal Revenue Service–Criminal Investigation (IRS–CI), the Federal Deposit Insurance Corporation (FDIC) and the U.S. Department of the Treasury OIGs, and other federal law enforcement to use their extensive and specialized expertise in white-collar financial fraud to develop cases prosecuted by U.S. Attorney’s Offices across the nation. When appropriate, our agents also work with state and local law enforcement and other governmental organizations. We conduct outreach with Board and Bureau supervision, legal, and enforcement groups, including the 12 Federal Reserve Banks that supervise financial institutions under delegated authority from the Board and regional Bureau supervision staff.

Headquarters


A large part of the work of Investigative Operations falls to the Special Investigative Unit.

The SIU is a dedicated team of agents with extensive experience working cases that pose a reputational risk to the Board or the Bureau, such as leaks of confidential information or employee misconduct. The SIU regularly updates the inspector general and, when appropriate, top Board and Bureau officials on important developments.

The SIU’s work is fast paced and demanding. The cases are complex, with more interviews, more evidence, and more progress reports than a normal investigation. Their work is a critical part of meeting our mission to promote economy, efficiency, and effectiveness and to prevent and detect fraud, waste, and abuse in the programs and operations of the Board and the Bureau.
Technical Operations includes the Electronic Crimes Unit and the OIG Hotline.

ECU agents can recover deleted or otherwise hidden information from just about any electronic device. Powerful hardware and software help agents find key data, sift through metadata, break encryption, and crack passwords. They’ve discovered crucial evidence that’s been used to help prosecute individuals who have committed crimes related to the programs and operations of the Board and the Bureau.

Not all the work is conducted in the lab. ECU agents can also execute search and seizure of computer evidence, write warrant applications for data, and provide onsite support to help bring equipment back to the lab so that they can recover evidence. They also refer potential security vulnerabilities to the Board and the Bureau and participate in the FBI’s Cyber Task Force and the U.S. Secret Service’s Cybercrimes Task Force.

To do this work, ECU agents undergo extensive specialized training in addition to standard law enforcement officer training. They work with the Federal Law Enforcement Training Center and the U.S. Department of Defense to sharpen their forensic skills.

The OIG Hotline helps people report fraud, waste, abuse, and mismanagement related to the programs or operations of the Board and the Bureau. Hotline staff can be reached by phone, web form, fax, or mail. We review all incoming hotline communications, research and analyze the issues raised, and determine how best to address the complaints.
Types of Cases

**Criminal cases**

*Criminal cases* are potential violations of law for which the penalties may include fines or incarceration—for example, a bank executive who obstructs the examination process or falsifies data or other information.

**Administrative cases**

*Administrative cases* typically involve agency employees whose potential misconduct may have violated a federal regulation or agency policy, for which penalties may involve administrative discipline. An example would be an employee who uses their government travel card in a manner that violates agency policy.

**Civil cases**

*Civil cases* generally involve potential violations of law for which the federal government’s remedies include the ability to recover monetary damages from the wrongdoer—for example, a contractor who submits a false claim, such as billing an agency for work that was never performed.

The OIG does not investigate violations of banking or consumer financial regulations. These matters are program operating responsibilities of the Board and the Bureau and are not within the OIG’s purview.

Process of Investigation

1. **Complaint evaluation**
2. **Preliminary investigation**
3. **Full investigation**
4. **Prosecution or administrative action**
Our Investigative Accomplishments

October 1, 2018–September 30, 2019

3 ARRESTS
6 CONVICTIONS

30 CASES CLOSED

$1.3B IN CRIMINAL FINES, RESTITUTION, AND SPECIAL ASSESSMENTS

17 MATTERS FOR PROSECUTORIAL CONSIDERATION
Case Highlights
October 1, 2018–September 30, 2019

We often work closely with the U.S. Department of Justice (DOJ), the FBI, and other law enforcement agencies. Investigative findings may be referred to DOJ for criminal prosecution or civil litigation or to the Board or the Bureau for administrative discipline or other actions.
The former general counsel for First NBC Bank, a New Orleans–based bank that failed in April 2017, was charged with conspiracy to commit bank fraud in the U.S. District Court for the Eastern District of Louisiana and pleaded guilty. The bank was a subsidiary of First NBC Bank Holding Company, a Board-supervised bank holding company.

The general counsel worked at First NBC Bank from about 2006 to 2016, during which time he and several businesses he owned or controlled received loans from the bank. A bank president, bank officer, and others conspired to provide First NBC Bank with fraudulent documents that overstated the value and understated liabilities of the general counsel’s and his businesses’ assets. These individuals also extended the maturity dates of the loans and issued new loans, including through straw borrowers, giving the appearance that older loans were paid to avoid the bank’s downgrading and reporting the loans as losses. In addition, the individuals funded fraudulent tax credit investments from the bank that were actually diverted to the general counsel and his businesses.

By April 2017, First NBC Bank had advanced about $46 million to the general counsel and his businesses. The bank also paid the general counsel an additional $9.6 million dollars in false tax credit investment money. If found guilty, the general counsel could face up to 30 years’ imprisonment, a fine of more than $1 million, 5 years’ supervised release, and a special assessment of $100.

Another individual, a borrower of First NBC Bank, was charged with and pleaded guilty to one count of conspiracy to commit bank fraud in the U.S. District Court for the Eastern District of Louisiana. According to the court documents, this defendant, at the direction of the same bank president, submitted false financial statements and inflated accounts receivable to justify incremental increases on a line of credit the defendant received from First NBC Bank. The president caused these false supporting documents to be placed in First NBC Bank’s records.

This conspiracy allowed the defendant, the president, and others to unjustly enrich themselves, disguise the defendant’s true financial status, and conceal the accurate performance of the defendant’s line of credit.

This conspiracy allowed the defendant, the president, and others to unjustly enrich themselves, disguise the defendant’s true financial status, and conceal the accurate performance of the defendant’s line of credit. The defendant, the president, and others sought to obtain money from First NBC Bank, in part so that the president could continue using the defendant on projects involving a company co-owned by the president without having to use the president’s funds to pay the defendant for work on the projects.

This is a joint investigation by our office, the FBI, and the FDIC OIG and is being prosecuted by the U.S. Attorney’s Office for the Eastern District of Louisiana.
Four former executives of Wilmington Trust Bank—the president and chief operating officer, the executive vice president and chief financial officer, the chief credit officer, and the controller—were sentenced in U.S. District Court for the District of Delaware. Two of the executives each received a sentence of 72 months’ incarceration, 3 years’ supervised release, a requirement to enter into a consent order with the Board for removal and prohibition from banking, and a fine of $300,000. One of the other executives received 54 months’ incarceration, 3 years’ supervised release, a requirement to enter into a consent order with the Board for removal and prohibition from banking, and a fine of $100,000. The remaining executive received 36 months’ incarceration and a requirement to enter into a consent order with the Board for removal and prohibition from banking.

The sentences were based on previous convictions by a jury that found all four defendants guilty of conspiracy to defraud the United States, securities fraud, making false statements in documents required to be filed with the U.S. Securities and Exchange Commission (SEC), making false entries in banking records, and making false statements to the SEC and to the Board. The jury also found the executive vice president and chief financial officer guilty of making false certifications in financial reports.

According to court documents, the bank was required to report in its quarterly filings with both the SEC and the Board the quantity of its loans for which payment was past due for 90 days or more. The defendants conspired to conceal the truth about the health of Wilmington Trust’s loan portfolio from bank regulators, the SEC, and the investing public. The defendants participated in Wilmington Trust’s failure to include in its reporting a material quantity of past-due loans, despite the reporting requirements and knowing the significance of past-due loan volume to investors and regulators.

This case was investigated by our office, the FBI, IRS–CI, and the Office of the Special Inspector General for the Troubled Asset Relief Program.
In total, SG engaged in more than 2,500 sanctions-violating transactions through U.S. financial institutions, causing it to process close to $13 billion in transactions that otherwise should have been rejected, blocked, or stopped for investigation pursuant to regulations promulgated by the Office of Foreign Assets Control.

On November 19, 2018, the U.S. Attorney’s Office for the Southern District of New York announced criminal charges against Société Générale (SG) consisting of a one-count felony information charging SG with conspiring to violate the Trading with the Enemy Act and the Cuban Asset Control Regulations for SG’s role in processing billions of dollars of U.S. dollar transactions using the U.S. financial system, in connection with credit facilities involving Cuba. The U.S. Attorney’s Office also announced a deferred prosecution agreement under which SG agreed to accept responsibility for its conduct by stipulating to the accuracy of an extensive Statement of Facts, pay penalties totaling $1.34 billion to federal and state prosecutors and regulators, refrain from all future criminal conduct, and implement remedial measures as required by its regulators. The $1.34 billion in penalties represents the second-largest penalty ever imposed on a financial institution for violations of U.S. economic sanctions.

From about 2004 to 2010, SG, in contravention of U.S. sanctions laws, operated 21 credit facilities that provided significant money flow to Cuban banks, entities controlled by Cuba, and Cuban and foreign corporations for business conducted in Cuba; those Cuban credit facilities involved substantial U.S.-cleared payments through U.S. financial institutions in violation of the Trading with the Enemy Act and the Cuban Regulations. In total, SG engaged in more than 2,500 sanctions-violating transactions through U.S. financial institutions, causing it to process close to $13 billion in transactions that otherwise should have been rejected, blocked, or stopped for investigation pursuant to regulations promulgated by the Office of Foreign Assets Control. Most of these transactions and most of the total value involved a U.S. dollar credit facility designed to finance oil transactions between a Dutch commodities trading firm and a Cuban corporation with a state monopoly on producing and refining crude oil in Cuba.

SG avoided detection, in part, by making inaccurate or incomplete notations on payment messages that accompanied these sanctions-violating transactions. Indeed, the SG department that managed many of the Cuban credit facilities engaged in a deliberate practice of concealing the Cuban nexus of U.S. dollar payments that were made in connection with those facilities. For example, SG routed about 500 U.S. dollar–denominated payments through a particular Spanish bank to disguise the fact that the transactions violated U.S. sanctions, and employees were instructed to omit any references to Cuba or Cuban entities from the messages that accompanied the fund transfers.

Despite the awareness of both SG’s senior management and Group Compliance that SG had engaged in this unlawful conduct, SG did not disclose its conduct to the Office of Foreign Assets Control or any other U.S. regulator, including the Board, or law enforcement agency until well after the government’s investigation began.

This investigation was conducted by our office and the IRS–CI and was prosecuted by the U.S. Attorney’s Office for the Southern District of New York.
Former Acting President of CFG Community Bank Sentenced to Federal Prison for Bank Fraud and Tax Evasion

According to court documents, the defendant diverted $100,000 in CFG funds for his own benefit... directed a settlement company to divert over $775,000 in loan proceeds for his personal benefit and the benefit of a friend... and diverted $91,126.56 in insurance premium refunds... to his personal account.

A former acting president of CFG Community Bank, a state member bank, was sentenced to 3 years in federal prison for bank fraud and tax evasion. The defendant was also ordered to pay $892,541.75 in restitution to CFG and $365,228.80 in restitution to the Internal Revenue Service and to forfeit $503,378.87.

According to court documents, the defendant diverted $100,000 in CFG funds for his own benefit while he was acting president. Later, while he was president of CFG affiliate Capital Financial Ventures, LLC, the defendant schemed to defraud CFG by posing as its current chief executive officer and president to refinance CFG-owned mortgage loans. He then directed a settlement company to divert over $775,000 in loan proceeds for his personal benefit and the benefit of a friend. The defendant created false correspondence with the loan borrowers to conceal the diversion from CFG. The defendant also diverted $91,126.56 in insurance premium refunds on one of the commercial loans purchased by CFG to his personal account instead of paying the funds over to the borrower.

In addition, in fall 2011 the defendant and codefendant attempted to realize a profit from a group of nonperforming mortgages their company, Capital T Partners Brookfield, LLC, had purchased by donating some of the mortgages to a charity and taking a charitable deduction on their income tax returns. The defendant admitted that he and the codefendant created a false Internal Revenue Service form 8283 and a false appraisal, which purported that the mortgages were valued at over $1 million. As a result, the defendant and the codefendant received a valuable tax deduction. The defendant also admitted that he failed to report income of more than $176,000 in 2010 and $480,000 in 2011. The defendant underpaid his taxes for 2010, 2011, and 2012 by $365,228.80.

This was a joint investigation by our office, the FBI, the IRS–CI, and the Social Security Administration OIG and was prosecuted by the U.S. Attorney’s Office for the District of Maryland.

Former Synovus Employee Pledged Guilty to Bank Fraud and Tax Evasion

The former employee diverted $1,046,602 in client funds to a personal account at another bank... [and] used these funds to pay for a wide assortment of his personal expenses.

A former commercial banker for Synovus Bank, a state member bank, pleaded guilty to four counts of bank fraud and four counts of tax evasion and was sentenced to 24 months in federal prison after he pleaded guilty to four counts of bank fraud and four counts of tax evasion. He was also ordered to pay restitution of $166,481 to Synovus and $221,357 to the Internal Revenue Service.

Between July 2, 2013, and May 24, 2017, while managing some of the bank’s largest clients, the defendant diverted $1,046,602 in client funds to a personal account at another bank. Financial records revealed that the defendant used these funds to pay for a wide assortment of his personal expenses, including payments on vehicles, credit card bills, vacations, jewelry, and cash withdrawals. In addition, the defendant failed to pay income taxes on the stolen money, amounting to $221,357.

This was a joint investigation by our office, the FBI, and the IRS–CI and was prosecuted by the U.S. Attorney’s Office for the Middle District of Georgia.
Wells Fargo and Co. and its subsidiary, Wells Fargo Bank, N.A., have agreed to pay $3 billion to resolve matters stemming from a years-long practice of pressuring employees to meet unrealistic sales goals. Wells Fargo admitted to this practice and that it collected millions of dollars in fees and interest to which the company was not entitled, harmed the credit ratings of certain customers, and unlawfully misused customers’ sensitive personal information.
Beginning in 1998, Wells Fargo increased its focus on sales volume and reliance on annual sales growth. A core part of this sales model was the cross-sell strategy—selling existing customers additional financial products.

Wells Fargo’s Community Bank, then the largest operating segment of Wells Fargo, implemented a volume-based sales model in which employees were directed and pressured to sell large volumes of products to existing customers, often with little regard to actual customer need or expected use. Onerous sales goals and management pressure led thousands of employees to engage in unlawful conduct—including fraud, identity theft, and the falsification of bank records—and unethical practices to sell products of no or little value to the customer.

Many of these practices were referred to within Wells Fargo as gaming. Customer signatures were forged to open accounts without authorization, PINs created to activate unauthorized debit cards, money moved from millions of customer accounts to unauthorized accounts, credit cards and bill pay products opened without authorization, customers’ contact information altered to prevent them from learning of unauthorized accounts, and customers encouraged to open accounts they neither wanted or needed.

Despite knowledge of the illegal sales practices, Community Bank senior leadership failed to prevent and reduce these practices. To Wells Fargo management and the board of directors, they cast the problem as driven by individual misconduct instead of the sales model itself.

“This settlement holds Wells Fargo accountable for tolerating fraudulent conduct that is remarkable both for its duration and scope, and for its blatant disregard of customers’ private information,” said Deputy Assistant Attorney General Michael D. Granston of DOJ’s Civil Division.

“Our office is committed to bringing to justice those who deliberately falsify and fabricate bank records in order to deceive regulators and the public,” said Inspector General Mark Bialek of the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection. “I commend our agents and our law enforcement partners for their hard work and persistence that led to today’s announcement.”

This case was the result of coordination among our office; DOJ, including multiple U.S. Attorney’s offices; the SEC; the FBI; the FDIC OIG; the Federal Housing Finance Agency OIG; and the United States Postal Inspection Service.
Teaming Up With Other Agencies to Solve Financial Crime Cases

How outreach, partnership, and collaboration lead to successful investigations

Financial crimes like bank fraud and loan fraud tend to be complex. The evidence for such crimes often includes tens of thousands of documents—bank statements, emails, Call Reports, text messages, loan files, and other records—which can be time consuming to analyze.
Criminal statute violations often fall within the jurisdiction of multiple agencies. To effectively investigate financial crimes, our special agents often collaborate with other agencies.

**Why We Work Together**

**Personnel.** We have field offices in Chicago, Miami, New York City, and San Francisco. Each field office has only a few agents, who each carry multiple cases and are responsible for several states. Because interviews are usually conducted with two agents, it’s helpful to work with another agency. Other agencies can also help with surveillance, undercover operations, and arrests, which may require additional personnel. And because agents sometimes work cases that are based several states away, it can be valuable to partner with an agent in the geographic vicinity of the person being investigated in order to better access local contacts and information.

**Access to technological resources.** Working together allows agencies to share technological resources. For example, the FDIC has resources to efficiently retrieve and search records from banks that have closed. We have a forensic analysis team that can retrieve records, emails, and text messages from computers, smart phones, and other electronic devices. Sharing resources helps us solve cases effectively and save money.

**Sharing expertise.** Special agents have diverse backgrounds and experiences that position them to contribute in varied ways. For example, some agents have financial backgrounds, while others are skilled at undercover operations or surveillance techniques. Agencies also have different types of resources, such as dedicated analysts, surveillance teams, and access to investigative systems or information. As one agent described it, everyone who is part of the investigative team contributes a piece of the puzzle to solve the crime.

**Referrals.** Sometimes a case doesn’t exactly fit what we do. Knowing agents at various agencies and understanding what kinds of cases fall into their jurisdiction makes it easier to provide and receive case referrals.

**Concurrent jurisdiction.** In many cases, several IGs have concurrent jurisdiction, so it makes sense to work together. For example, while a bank may be supervised by a Reserve Bank, the FDIC may also have concurrent jurisdiction because of the Deposit Insurance Fund (the fund that pays back depositors after a bank fails). Cases of loan fraud may also involve the U.S. Small Business Administration or Federal Housing Finance Agency OIGs.

**Building Collaborative Relationships**

Our collaborative relationships with other agencies are essential to our work, and we prioritize building and maintaining these relationships through outreach. For example, our Chicago field office cohosts the Illinois Fraud Working Group with the U.S. Attorney’s Office Northern District of Illinois. The quarterly meetings, attended by financial OIGs, federal regulators, and other federal law enforcement, provide an opportunity to discuss cases and trends. In addition, the Chicago and San Francisco field offices often schedule their quarterly firearms training with other agencies as an opportunity to share resources and build relationships.

We also maintain collaborative relationships with staff within the Board, the Bureau, and the Reserve Banks, like bank examiners, who are essential to solving cases. These experts can provide firsthand knowledge that can make them a key witness in a case.

Of course, collaboration can be challenging. Agents travel frequently, and coordinating plans can be difficult. In addition, an agency’s priorities can change at any time, so an agent may be required to abruptly switch to a different case. But dealing with the drawbacks is clearly worth it.

**Collaboration Pays Off**

Many of our recent cases were solved through collaboration.

**Wilmington Trust Bank.** In 2018, four former executives of Wilmington Trust Bank were found guilty of conspiracy to defraud the United States, securities fraud, making false statements in documents required to be filed with the SEC, making false entries in banking records, and making false statements to the SEC and to the Board. They were sentenced to incarceration ranging from 36 to 72 months, a total of $700,000 in fines, and prohibition from banking. We worked on this case with the FBI, the Office of the Special Inspector General for the Troubled Asset Relief
Program, and the IRS–CI.

**CFG Community Bank.** In another recent case, the former acting President of CFG Community Bank, a state member bank, diverted more than $900,000 in funds for his own benefit. After pleading guilty to one count of bank fraud and one count of income tax evasion, he was sentenced to 3 years in federal prison. This was a joint investigation by our office, the FBI, the Social Security Administration OIG, and the IRS–CI and was prosecuted by the U.S. Attorney’s Office for the District of Maryland.

**Société Générale S.A.** And in a third case, Société Générale paid $1.34 billion in penalties for conspiring to violate the Trading with the Enemy Act—the second-largest penalty ever imposed on a financial institution for violations of U.S. economic sanctions. We conducted this investigation with the IRS–CI; the case was prosecuted by the U.S. Attorney’s Office for the Southern District of New York.

**Fighting Financial Crime**

Financial crimes aren’t just a matter of money. Although such crimes may seem abstract and victimless, they generate costs and consequences at a real, human level. Financial crimes often cause banks to close, which can have a communitywide effect, especially in rural areas. A recent Federal Reserve report found that when bank branches close, accessing financial services becomes more expensive and less convenient, especially for small business owners, older people, and those who have lower incomes and less reliable access to transportation. These effects can reverberate through the entire community.

Our work not only helps bring those who commit crimes to justice, but also deters crime by sending a clear message that there will be consequences for such crimes. We could not work as effectively and efficiently without the help of other agencies. Ultimately, collaboration helps the Office of Investigations achieve the OIG’s mission—to improve economy, efficiency, and effectiveness, and to prevent and detect fraud, waste, and abuse.
Training for OIG Special Agents

What happens when institutions provide false documents to Board or Bureau examiners or an examiner takes a bribe to look the other way? Or when an employee uses agency information—like confidential financial data—for personal gain? OIG special agents are trained to investigate.
White-collar crime investigations involve myriad law enforcement skills that special agents develop through years of training and experience. In fact, an OIG special agent’s training never ends.

The OIG hires new special agents as well as special agents from other government agencies who may already have years of law enforcement experience. Special agent candidates must meet a set of physical requirements, such as having good vision and hearing. They also must be under 37 years old and have a bachelor’s degree. Most important, before new hires can become special agents, they must successfully complete a comprehensive federal training course in criminal investigation.

### Criminal Investigator Training Program: Law Enforcement Basics

All special agents are required to pass an 11-week course called the Criminal Investigator Training Program (CITP) through the Federal Law Enforcement Training Centers (FLETC). CITP is held on the FLETC campus in Glynco, Georgia, and incorporates lectures, laboratory work, practical exercises, and written exams to teach arrest and search techniques, self-defense, marksmanship, and other skills. In addition to CITP, newly hired first-time agents also take an OIG-specific course, while current Special Agents participate in a shorter transitional training.

During CITP, trainees work a simulated case—for example, an allegation that computers have been stolen and are being sold online—and use that case to practice skills they are learning, including interviewing suspects and witnesses, performing surveillance and undercover operations, writing and executing search and arrest warrants, writing a criminal complaint, obtaining an indictment, and testifying in a courtroom hearing. Agents must learn not only how to work within the parameters of the law, but also how to protect themselves when people don’t comply with lawful commands.

Most federal law enforcement agencies send their special agents to CITP (some agencies, like the FBI and the Drug Enforcement Administration, are large enough to have their own training programs). Living and training alongside investigators working for other agencies helps special agents make contacts and build relationships that can be useful throughout their careers. Many special agents enjoy the camaraderie that develops among the trainees.

Trainees must endure paramilitary-style training, including living in dorms, wearing uniforms, adhering to regimented schedules, running in cadence, and embracing a team mentality. They must also balance the academic course load and physical demands with the challenges that come from being away from home for several months. Getting through the program requires commitment, mental and physical toughness, and grit.

### IG Investigator Training Program: OIG-Specific Training

Within their first year of OIG employment and within 3 to 6 months of completing CITP, special agents take the Council of the Inspectors General on Integrity and Efficiency’s IG Investigator Training Program. In this 3-week course, also held in Glynco, Georgia, special
agents learn how to apply the framework of legal considerations and tactical training to the OIG environment. They also learn about the authorities, duties, responsibilities, and obligations associated with the Inspector General Act of 1978, as amended. Topics covered include IG subpoenas, employee misconduct investigations, and government workplace searches, among many others.

**Specialized Training: Developing Expertise**

Many special agents also pursue specialized training in areas such as computer forensics; undercover operations; firearms; and control tactics, a term for defensive tactics that emphasize proactive physical control of the situation. These specialized training classes can be weeks or months long. Other special agents have developed expertise in bank fraud, money laundering, the Bank Secrecy Act, or other financial topics. Many OIG special agents are also qualified to teach specialized training courses.

Having special agents who specialize in different areas ensures that the OIG will be prepared to investigate a variety of cases. For example, if a special agent is interviewing a banker, the agent must have enough subject-matter knowledge to understand whether the banker’s responses make sense and to know which follow-up questions are appropriate.

**Ongoing Training: Maintaining Skills and Knowledge**

Special agents also complete a variety of ongoing training assignments. Every quarter, for example, special agents must pass a firearms training that involves a qualification course for several firearms and long guns. Special agents must achieve a certain accuracy score each time.

Special agents also undergo annual training on several topics, including flying armed on airplanes, safety around blood-borne pathogens, and ethics. Every 3 years, special agents take additional training on a variety of topics, including a legal refresher course, first aid and CPR, physical conditioning and defensive tactics, arrest techniques, and intermediate weapons.

Ongoing training can be time intensive, but it’s important to stay up to date on laws and law enforcement practices, which change periodically. Training also ensures that special agents maintain the skills and knowledge that they might not use regularly. And while the training covers a wide range of topics, this scope reflects the extensive skill set required by the job.

**Meeting Evolving Demands**

The financial and regulatory environment is always changing, so special agents must also grow and ensure that they have the right skills and mindset to meet evolving demands. In interviews, special agents emphasized how having a mindset of constantly striving to improve and ensuring that they were well prepared helped them succeed—and stay safe—on the job. Ultimately, training builds the foundation of skills and knowledge special agents need to help the OIG combat fraud, waste, and abuse.
More About the OIG

**Information Technology**
IT auditors conduct audits and evaluations of the economy, efficiency, and effectiveness of the IT programs and systems of the Board and the Bureau. These audits focus on information security controls, systems development, operations, investment, and contractor support. IT staff also provide data analytics support for audits, evaluations, and investigations.

**Audits and Evaluations**
Auditors conduct audits and evaluations of the economy, efficiency, and effectiveness of the programs and operations of the Board and the Bureau; the agencies’ compliance with applicable laws and regulations; the effectiveness of their internal controls; and the presentation and accuracy of the Board’s and the Federal Financial Institutions Examination Council’s financial statements.

**Front Office**
Front office staff plan and execute our strategic direction; manage communications; execute our internal quality assurance function; provide general support for our IT infrastructure; and provide administrative and human resources services.

**Legal Services**
Attorneys advise the inspector general and staff on all legal matters and provide strategic analysis, counseling, research, and representation. Legal staff also conduct legislative and regulatory reviews and manage congressional and media relations.
OIG Hotline

Help the Board and the Bureau work efficiently; effectively; and free of fraud, waste, and abuse.

What should I report?

- Violations of federal laws or agency policies
- Contract and procurement irregularities
- Travel card or purchase card fraud
- Ethics violations or conflicts of interest by agency officials
- Employee misconduct
- Theft or abuse of property
- Obstruction of agency operations, such as providing false information to regulators
- Waste or mismanagement of funds or government resources

How do I report?

- oig.federalreserve.gov/hotline
- oig.consumerfinance.gov/hotline
- 1-800-827-3340
- Board of Governors of the Federal Reserve System
  20th Street and Constitution Avenue NW
  Mail Stop K-300
  Washington, DC 20551

Am I protected?

We will not disclose your identity except in rare circumstances where it’s unavoidable. Further, Board and Bureau employees are protected by law from reprisals or retaliation for contacting us. Reserve Bank staff should refer to their Reserve Bank policy.