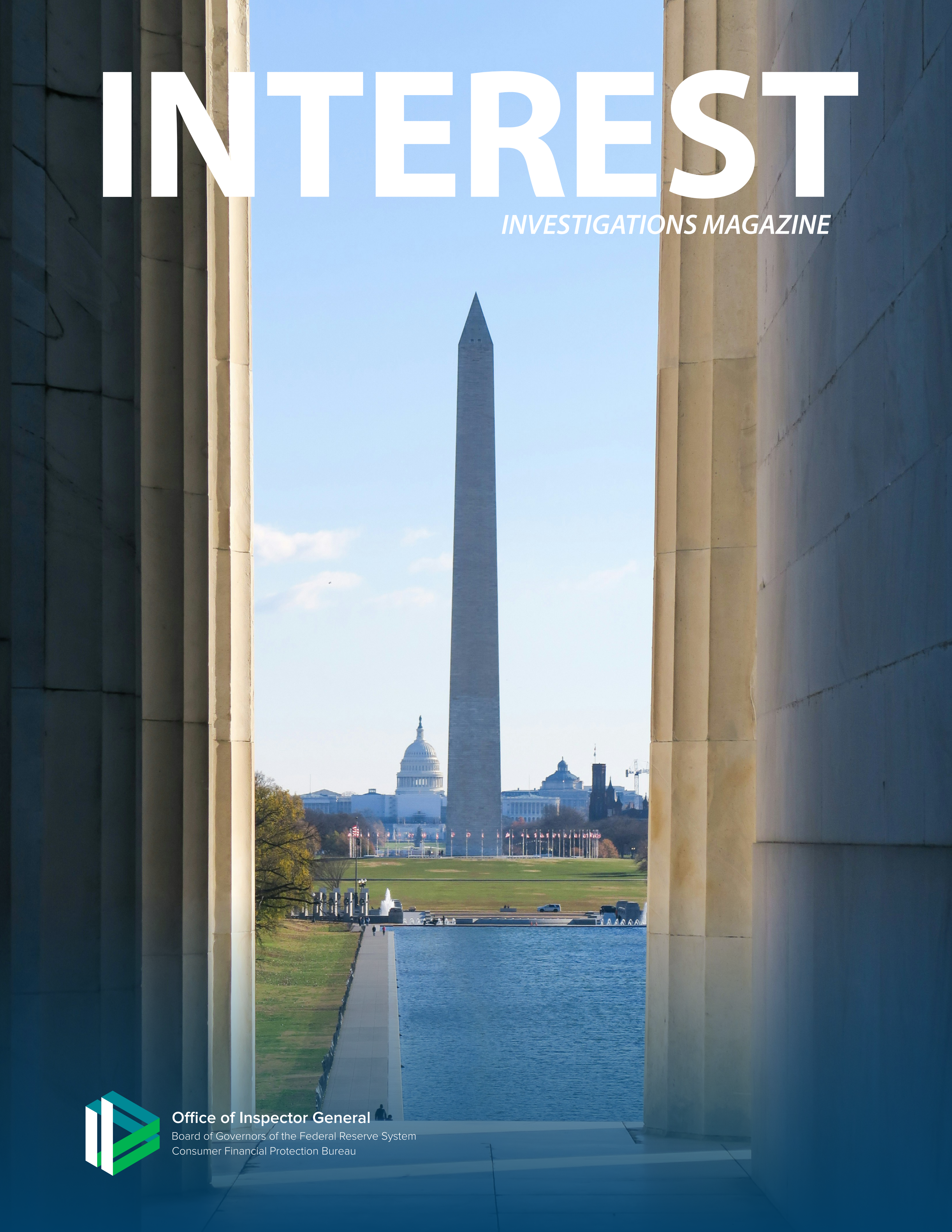
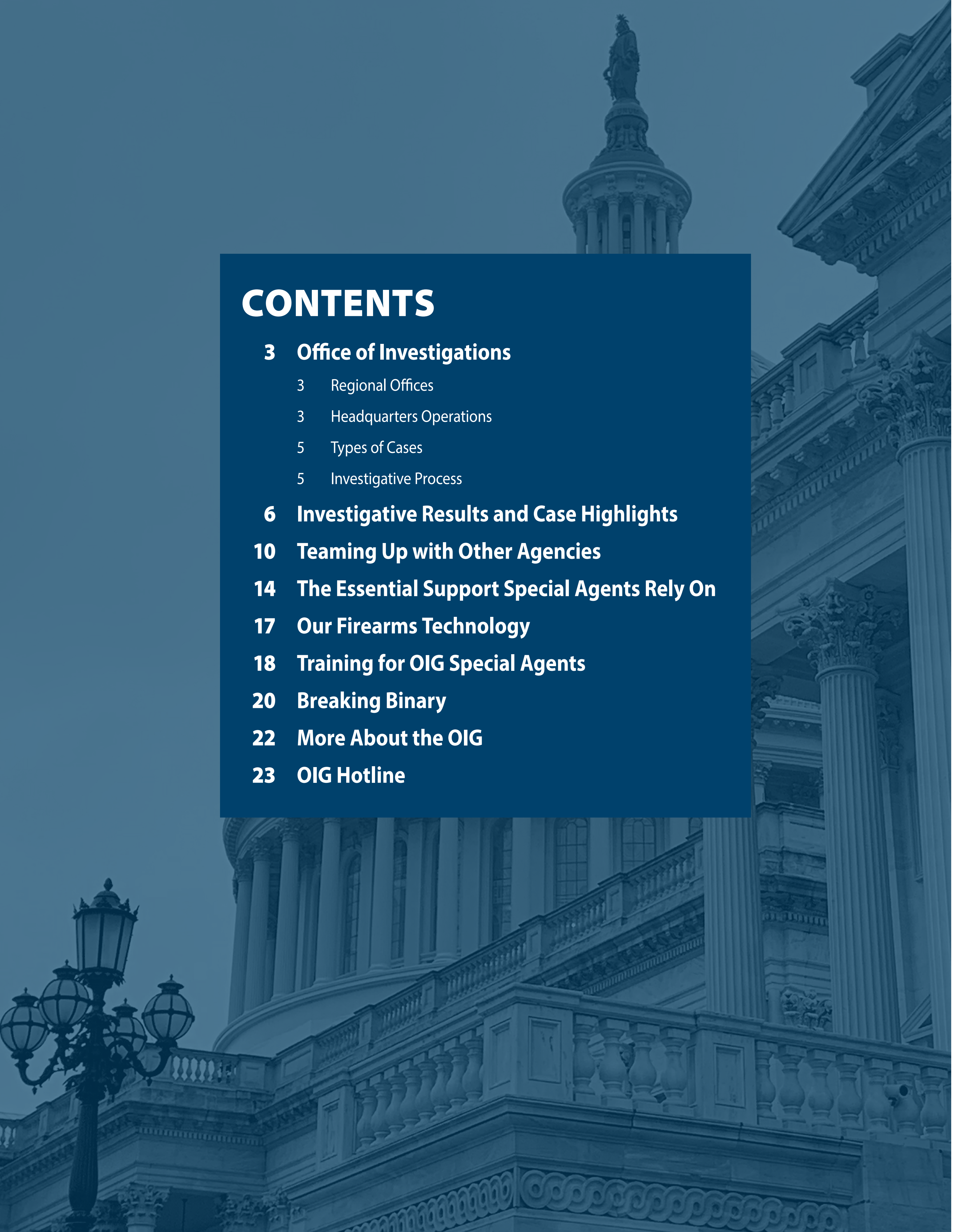
INTEREST

INVESTIGATIONS MAGAZINE



Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau



CONTENTS

OFFICE OF INVESTIGATIONS

Our investigative team includes federal special agents, forensic analysts, technical specialists, and support staff with a broad range of experience. Our special 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, U.S. attorney's offices, and state and local law enforcement, adding value to complex investigations by virtue of our specialized knowledge and experience.

REGIONAL OFFICES

Our regional offices are Chicago (Midwestern Region); Miami (Southeastern Region); New York City (Northeastern Region); San Francisco (Western Region); and Headquarters/Washington, DC (Mid-Atlantic Region).

The regional offices partner with the Federal Bureau of Investigation (FBI), the U.S. Secret Service, the Internal Revenue Service (IRS) Criminal Investigation (CI), the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General, the U.S. Small Business Administration (SBA) Office of Inspector General, the Special Inspector General for Pandemic Recovery (SIGPR), and other federal law enforcement, using their extensive specialized expertise in white-collar financial fraud to develop cases prosecuted by U.S. attorney's offices across the nation. When appropriate, our special agents also work with state and local law enforcement and other governmental organizations. We conduct outreach with the supervision, legal, and enforcement groups at the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau, including the 12 Federal Reserve Banks that supervise financial institutions under delegated authority from the Board and regional CFPB supervision staff.

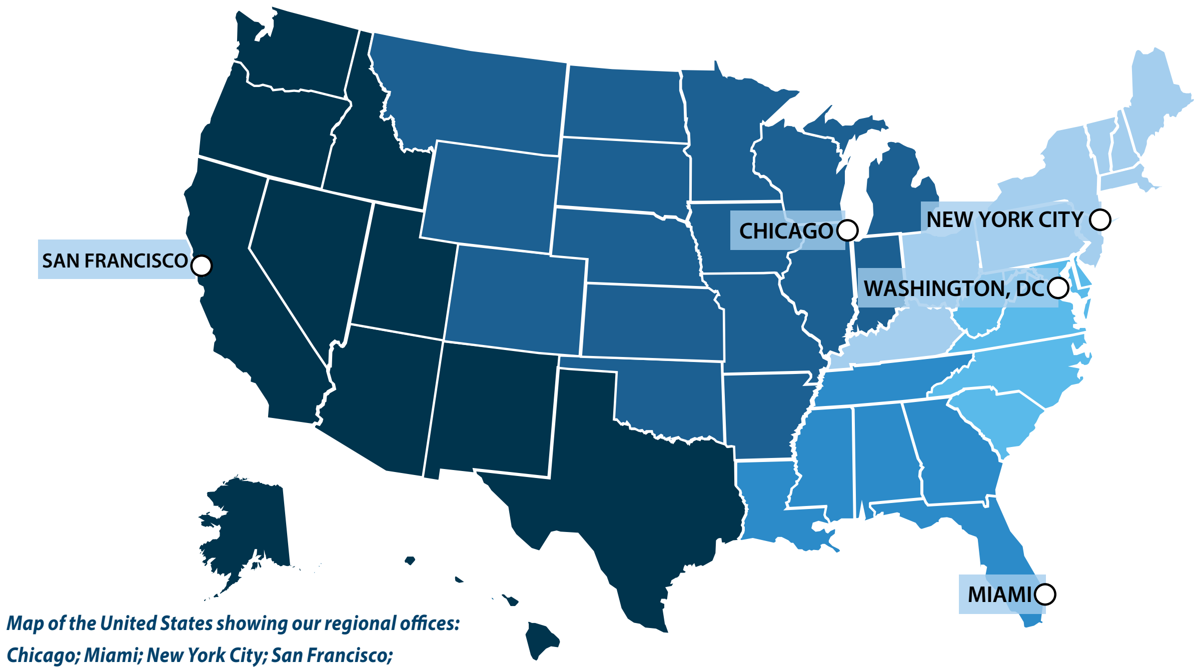
HEADQUARTERS OPERATIONS

Headquarters Operations, located in the Headquarters/Washington, DC, regional office, oversees all regional offices and provides operational and administrative support. Headquarters Operations comprises the Special Investigations Unit (SIU), the Electronic Crimes Unit (ECU), the OIG Hotline, and the Investigative and Administrative Support team.

Special Investigations Unit

The SIU performs a large percentage of the investigative work at the Headquarters/Washington, DC, regional office. The SIU is a dedicated team of special agents with extensive experience working cases that pose a reputational risk to the Board or the CFPB, such as leaks of confidential information or employee misconduct. The SIU regularly updates the inspector general (IG) and, when appropriate, top Board and CFPB officials on important developments.

The SIU's work is fast paced and 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 CFPB.



Map of the United States showing our regional offices: Chicago; Miami; New York City; San Francisco; and Headquarters/Washington, DC.

Electronic Crimes Unit

The ECU serves as the digital forensic investigative unit of the OIG. The ECU is responsible for providing detailed, complex analysis of electronic data associated with OIG investigations. The ECU uses specialized computer hardware and software to help special agents find key data, sift through metadata, break encryption, and crack passwords. Our special agents have discovered crucial evidence that has been used to help prosecute individuals who have committed crimes related to the programs and operations of the Board and the CFPB. Not all the work is conducted in the lab. ECU special 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.

The ECU participates in the FBI's Cyber Task Force and the U.S. Secret Service's Cybercrimes Task Force and adheres to computer forensic quality assurance standards as directed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Hotline

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

Investigative and Administrative Support

The Investigative and Administrative Support function conducts financial analysis and policy development and review; handles budgeting and procurement; coordinates firearms training, defensive tactics training, and other training; handles internal and external peer reviews, Freedom of Information Act inquiries, and congressional inquiries; manages and administers the investigative case management system; and delivers statistical reporting to Congress, the U.S. Department of Justice (DOJ), the U.S. attorney general, and CIGIE.

TYPES OF CASES

CRIMINAL

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

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

CIVIL

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.

We do not investigate violations of banking or consumer financial regulations. These matters are program operating responsibilities of the Board and the CFPB.

INVESTIGATIVE PROCESS

COMPLAINT EVALUATION

Incoming complaints initially undergo a limited evaluation to identify whether the potential violation is within our jurisdiction (typically 30 days).

PRELIMINARY INVESTIGATION

A preliminary investigation is a deeper evaluation of allegations of potential criminal activity during which ambiguous or incomplete information is clarified (typically 180 days). All lawful investigative methods may be used in a preliminary investigation except for electronic surveillance, physical searches, and acquisition of foreign intelligence information.

FULL INVESTIGATION

A full investigation is undertaken when an articulable, factual basis has been established that reasonably indicates that a federal crime may have been committed. All lawful investigative methods may be used in a full investigation.

PROSECUTION OR ADMINISTRATIVE ACTION

Prosecution involves formal charges by the U.S. Attorney's Office that may lead to an indictment, trial, conviction, or guilty plea; administrative action may lead to oral or written reprimands, suspension, debarment, or termination.

INVESTIGATIVE RESULTS AND CASE HIGHLIGHTS

FORMER FIRST NBC BANK PRESIDENT SENTENCED IN LOUISIANA TO 14 YEARS IN PRISON AND $214 MILLION RESTITUTION FOR FRAUD THAT CAUSED BANK'S FAILURE

For his role in a fraud scheme leading to the failure of the $5 billion First NBC Bank, Ashton J. Ryan Jr., former president and CEO, was sentenced to 170 months in prison after being convicted of all 46 counts against him, including bank fraud, conspiracy to commit bank fraud, and making false entries in bank records. He was also sentenced to 3 years of supervised released and ordered to pay $214 million in restitution. Based in New Orleans, the bank was a subsidiary of the Board-supervised First NBC Bank Holding Company. The bank's failure cost the FDIC's Deposit Insurance Fund just under $1 billion.

In the long-running scheme, Ryan and several other executives conspired with borrowers to defraud the bank. The executives extended loans to the borrowers, who were unable to repay the loans, and then extended new loans to the borrowers to cover the existing loans. Ryan and the executives enriched themselves through fees earned on the loans while concealing their actions—and the true financial condition of the bank—from the board of directors and outside auditors and examiners. By the time the bank collapsed, these bogus loans totaled hundreds of millions of dollars.

We conducted this investigation with the FBI and the FDIC Office of Inspector General. The U.S. Attorney's Office for the Eastern District of Louisiana prosecuted.

FORMER SENIOR MANAGER OF FRB RICHMOND SENTENCED FOR INSIDER TRADING AND MAKING FALSE STATEMENTS

Robert Brian Thompson, of Virginia, was sentenced to 24 months in prison with 24 months of supervised release and ordered to forfeit $771,678. Thompson pleaded guilty to misappropriating confidential information to execute trades in publicly traded financial institutions.

Thompson, who worked as a bank examiner and senior manager at FRB Richmond, misappropriated confidential information, including confidential supervisory information, to execute trades in publicly traded financial institutions. Over several years, Thompson made 69 trades of seven publicly traded financial institutions, which resulted in over $771,000 in personal profits. To conceal the scheme, Thompson falsely represented on his required annual financial disclosures that he had no assets, including no equities in any publicly traded financial institutions, and that he had not engaged in any activity that would constitute conflicts of interest, violations of FRB Richmond policies, or violations of law.

The DOJ and the U.S. Attorney's Office for the Eastern District of Virginia prosecuted this case.

CEO OF MBE CAPITAL SENTENCED IN NEW YORK TO 54 MONTHS IN PRISON AND RESTITUTION FOR $823 MILLION PANDEMIC FRAUD

Rafael Martinez, CEO and primary owner of MBE Capital Partners, was sentenced to 54 months in prison for conspiracy to commit wire fraud in connection with an $823 million Paycheck Protection Program (PPP) loan and lender fraud scheme. He was also sentenced to 3 years of supervised release and ordered to pay over $71 million in restitution and forfeit nearly $45 million along with multiple properties and luxury vehicles.

Martinez used false representations and documents to fraudulently obtain SBA approval for his company, MBE Capital Partners, to be a nonbank PPP lender. After MBE was approved, Martinez issued $823 million in PPP loans to about 36,600 businesses. Those loans earned Martinez over $71 million in lender fees. In addition, Martinez schemed to obtain a PPP loan of over $283,000 for MBE through false statements about employees and wages using the forged signature of MBE's tax preparer. Martinez spent the proceeds from his criminal conduct on, among other things, a $10 million villa in the Dominican Republic; a $3.5 million mansion in New Jersey; a chartered jet service; and several luxury vehicles, including a Bentley, a BMW, a Ferrari, a Mercedes-Benz, and a Porsche.

We conducted this investigation with the IRS CI and the SBA Office of Inspector General. The U.S. Attorney's Office for the Southern District of New York prosecuted.

FORMER CEO OF FAILED KANSAS BANK SENTENCED TO PRISON FOR EMBEZZLING $47 MILLION

Shan Hanes was sentenced to 293 months in prison for embezzling $47.1 million from Heartland Tri-State Bank as its CEO. The embezzlement caused Heartland, a state member bank serving rural Kansas, to fail, with the FDIC absorbing the $47.1 million loss.

Hanes embezzled the money to enrich himself in a pig butchering cryptocurrency scheme. In this type of scheme, would-be investors are conned into depositing money into fake accounts controlled by the scammers. The scammers fabricate returns to encourage further deposits, then disappear with the money once the accounts are sufficiently "fattened up." Wielding his personal influence to circumvent Heartland's internal controls, Hanes effected wire transfers totaling $47.1 million in bank funds to buy cryptocurrency. The loss of assets significantly impaired Heartland's capital and liquidity, and the bank became insolvent.

We investigated this case with the FBI, the FDIC Office of Inspector General, and the Federal Housing Finance Agency Office of Inspector General. The U.S. Attorney's Office for the District of Kansas prosecuted.

TEAMING UP WITH OTHER AGENCIES TO FIGHT FINANCIAL CRIME

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. Moreover, 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 regional offices in Chicago; Miami; New York City; San Francisco; and Washington, DC. Each regional office carries multiple cases and is responsible for several states. Interviews are usually conducted with two agents, and we leverage our relationships with partner agencies when needed. Other agencies often assist 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 OIGs 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 SBA or Federal Housing Finance Agency Offices of Inspector General.

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 regional office cohosts the Illinois Fraud Working Group with the

U.S. Attorney's Office for the Northern District of Illinois. This group meets several times per year; the meetings, attended by financial offices of inspector general, federal regulators, and other federal law enforcement, provide an opportunity to discuss cases and trends. In addition, the Chicago and San Francisco regional offices occasionally 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 CFPB, 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 the benefits clearly outweigh the drawbacks.

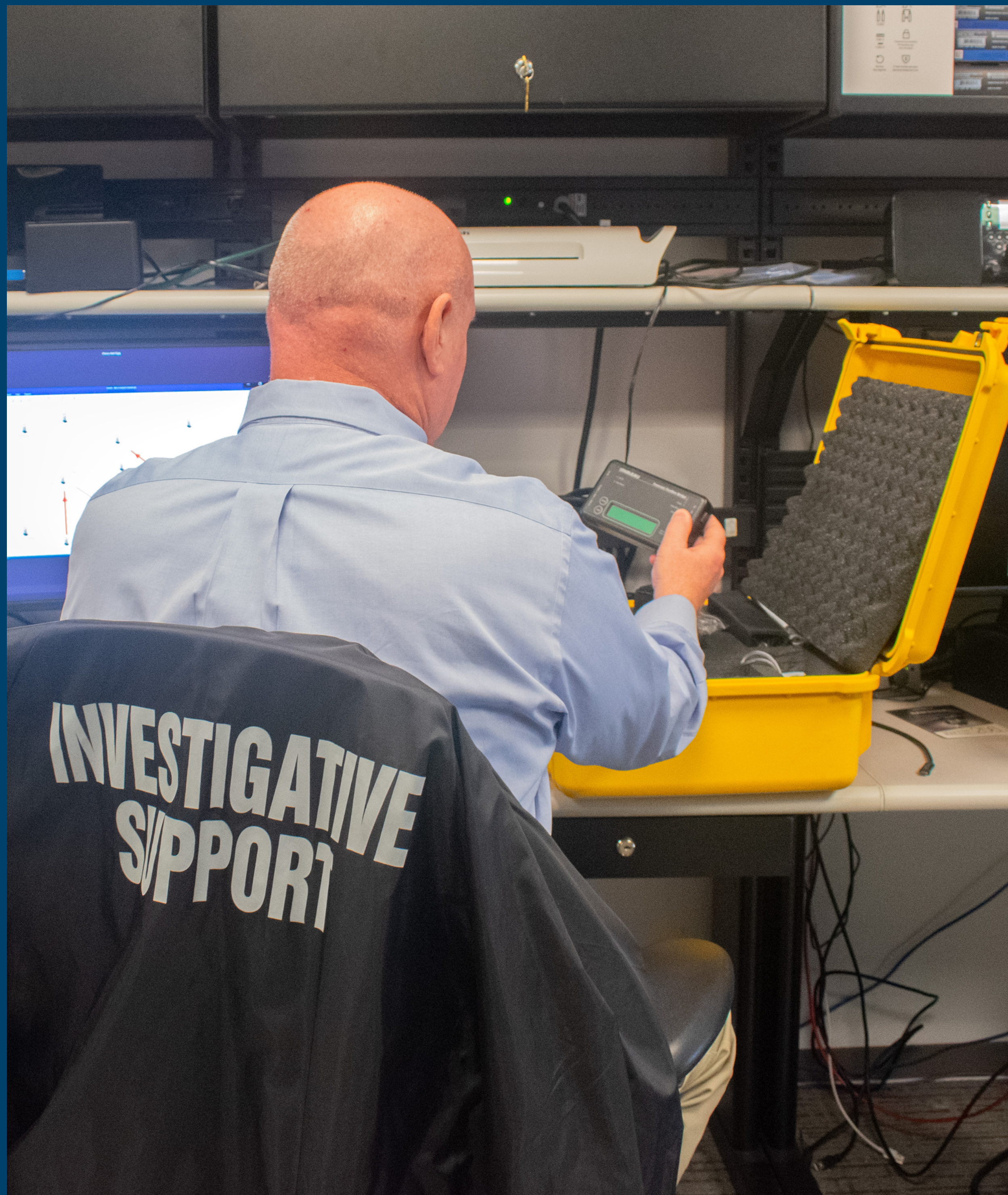
Agency OIGs We Collaborate With

Federal Bureau of Investigation
Federal Deposit Insurance Corporation Federal
Housing Finance Agency
Internal Revenue Service
U.S. Department of Treasury
U.S. Small Business Administration

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.



THE ESSENTIAL SUPPORT SPECIAL AGENTS RELY ON

Headquarters Operations is home to an important cadre of law enforcement professionals—investigative analysts (IAs). IAs support Headquarters Operations and our overall investigative operations by proactively searching for new cases, preparing analysis and documentation on active cases, and assisting with interviews and database lookups. IAs help prepare for proffers and organize documents for e-discovery. IAs also provide recommendations for actions, solutions, or alternatives based on research and analysis and knowledge of policies, procedures, and best or past practices, and they prepare written correspondence, reports, and briefs to report out on their work.

IAs contribute importantly to our investigations. Some recent examples include the following:

When a senior special agent was tasked by DOJ attorneys with locating 500 witnesses across the United States with only their names and prior employer name to go on, one of our IAs stepped up, conducted extensive social media research, and was able to locate 90 percent of the witnesses—far exceeding what any of the other agencies working the case were able to accomplish. This IA was commended by both DOJ attorneys and agents from other agencies assigned to the case. Thanks to the IA's efforts, the investigative team was able to contact numerous high-value witnesses.

Another case was discovered by one of our IAs during self-initiated work to support the OIG's mission. The IA worked closely with our senior special agents throughout the life of the case, helping to prepare and serve grand jury subpoenas and reviewing all responsive documents. The IA used forensic accounting to analyze commercial loan transactions in which the defendant fraudulently retained proceeds that were intended for various financial institutions he worked for. The IA traced the flow of fraudulent proceeds through various accounts and identified a multitude of ways in which the proceeds were used for personal gain. The IA helped to ultimately identify that the defendant embezzled $7.4 million from his financial institution employers.

On a complex Coronavirus Aid, Relief, and Economic Security Act loan case involving multiple financial institutions, one of our IAs created a Comprehensive Financial Investigative Solution (CFIS) analysis to capture and organize a large volume of bank data to assist in tracing loan proceeds. CFIS is a purpose-build financial investigative system for use by federal, state, and local prosecutors, law enforcement, regulatory agencies, and forensic accountants to perform rapid assembly and data capture of voluminous financial records and to automate the analysis of complex investigations for a full range of illicit financial schemes and frauds. The IA's efforts and expertise helped further the investigation by enhancing visibility into the flow of funds.

OIG IAs have at least a bachelor's degree in law enforcement, business administration, accounting, or a similar area; assistant IAs must have a high school diploma and 3 years of college. Certifications such as certified fraud examiner or certified public accountant are a plus. Successful IAs are skilled in data analytics, financial analysis, advanced research, and document review, among other areas. IAs must have strong written and oral communication skills; be critical thinkers; pay attention to details; collaborate well with colleagues; understand relevant laws and regulations; and know sources of information and the methods and techniques used to extract, analyze, and target useful data.

A variety of organizations offer training that is relevant to IAs, including the Federal Law Enforcement Training Center (FLETC), CIGIE, the International Association of Law Enforcement Intelligence Analysts, and the National Advocacy Center.

OUR FIREARMS TECHNOLOGY

The Office of Investigations stays up to date on technological improvements and trends in law enforcement and the firearms industry. Our most recent improvements were to our handguns and our optics.

LIGHTER HANDGUNS

We've procured lighter handguns, which makes them easier to operate and less burdensome to carry. Special agents carry a handgun for up to 12 hours a day, so a lighter firearm can make a big difference.

RED DOT SIGHTS

We use red dot sights, which create an illuminated red dot on the target that's only visible to the user. These optics provide several advantages over traditional iron sights, which require the user to visually align the front and rear sights. Red dot sights help special agents acquire the sight of the target more quickly, and they also improve accuracy for long-range shots. In addition, unlike traditional sights, which require users to shift their focus, special agents who are using red dot sights can keep both eyes open and on the target. Follow-up shots are also more accurate with red dot sights, and red dot sights are more effective than traditional sights in low-light environments. As a result of these advantages, red dot sights increase officer safety during critical incidents.

TRAINING FOR UPDATED FIREARMS TECHNOLOGY

While our handguns and optics are generally considered easier to use than the technology they replaced, any new technology comes with a learning curve. Our firearms instructors attended red dot instructor schools to prepare them to implement our conversion to red dot sights, and special agents underwent dedicated training on our new firearms equipment in addition to completing their required firearms qualifications every quarter. Special agents with additional responsibilities—such as operating rifles, which may be used during law enforcement operations with a potentially heightened risk or during other critical incidents—complete additional specialized training.

HELPING SPECIAL AGENTS SAFELY ACCOMPLISH OUR MISSION

In addition to providing ongoing training for our special agents, we continually research and evaluate technological developments and trends in the law enforcement community. While our tools and technology change over time, our goal remains the same: to prepare our special agents to carry out their work safely and effectively.

TRAINING FOR OIG SPECIAL AGENTS

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.

SPECIAL AGENT CANDIDATES

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 importantly, 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 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 special 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. Special 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 CIGIE 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 is 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 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.

BREAKING BINARY: INSIDE THE ELECTRONIC CRIMES UNIT

Allegations of fraud and other wrongdoing are hardly black-and-white issues when we first get them. But they are almost always binary.

"Everything happens electronically," says the head of our Electronic Crimes Unit. It's a simple statement that belies the complexity of the work of the ECU's digital forensics agents, who find evidence bit by bit, 1 by 0.

In the ECU lab, screens flash as OIG computer equipment noisily processes terabytes of data. The guts of computers, smartphones, servers, and other devices fill the room; if they are not being carefully inspected by agents, they sit neatly in evidence bags.

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 people who have committed crimes involving the programs and operations of the Board and the CFPB.

Not all the work is conducted in the lab. ECU agents can also execute search and seizure of computer evidence, write warrant requests for data, and provide onsite support to help bring equipment back to the lab so that they can recover evidence. They also support audits and refer potential security vulnerabilities to the Board and the CFPB.

To do this work, ECU agents undergo extensive specialized training in addition to standard law enforcement officer training. They work with FLETC and the U.S. Department of Defense to sharpen their forensic skills. They also participate in the FBI's Cyber Task Force and the U.S. Secret Service's Cybercrimes Task Force.

Having an internal lab leads to shorter turnarounds for forensic results. The lab also allows us to use cutting-edge forensics as a tool 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 CFPB.

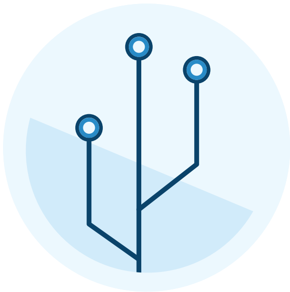
MORE ABOUT THE OIG

AUDITS AND EVALUATIONS

Auditors conduct audits and evaluations of the economy, efficiency, and effectiveness of the programs and operations of the Board and the CFPB; 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, coordinate our pandemic oversight work, lead outreach and engagement efforts, execute our internal quality assurance function, and provide general support for our information technology (IT) infrastructure.



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 CFPB. 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.

LEGAL SERVICES

Attorneys advise the IG 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.

MANAGEMENT, STRATEGIC COMMUNICATION, AND POLICY

Staff in this office provide administrative, communications, and human resources support to the entire OIG.

OIG HOTLINE

Help the Board and the CFPB 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

AM I PROTECTED?

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

WHAT HAPPENS AFTER I REPORT?

We evaluate the complaint and, if appropriate, refer our findings to the Board or the CFPB for administrative action (for example, taking personnel action against the offender) or to the DOJ for criminal or civil action.

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 Center I-2322
Washington, DC 20551

HOTLINE

INTEREST

INVESTIGATIONS MAGAZINE

Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

OIG Hotline
Report fraud, waste, or abuse.
oig.federalreserve.gov/hotline | oig.consumerfinance.gov/hotline
1-800-827-3340

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau