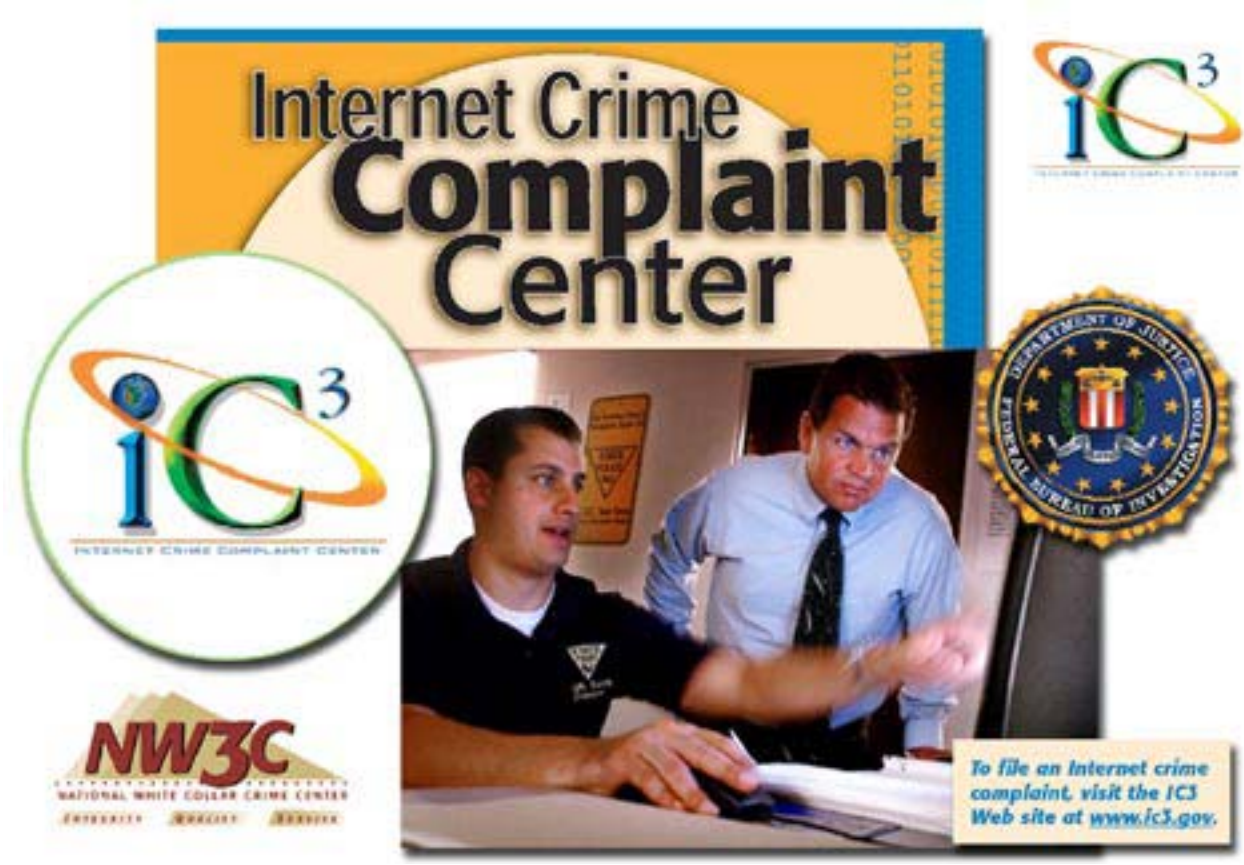


Fighting Online Crime

DANIEL LARKIN

Commerce online has brought crime online. Law enforcement agencies have developed new methods and new relationships to catch the bad guys in cyberspace.

Daniel Larkin is unit chief of the Internet Crime Complaint Center (IC3) at the U.S. Federal Bureau of Investigation (FBI).

Photo montage: The FBI's Internet Crime Complaint Center (IC3) is a clearinghouse for individuals' reports of illegal online activities. IC3 connects information from, perhaps, hundreds of victims of the same scam and builds a substantial case for law enforcement agencies to pursue. (Photograph from AP/Wide World Photos; Logos courtesy Internet Crime Complaint Center)

The Internet Crime Complaint Center (IC3) is a reporting and referral system for Internet crime complaints from people in the United States and around the world. Through an online complaint form and a team of agents and analysts, IC3 serves the public and U.S. and international law enforcement agencies investigating Internet crime.

Internet crime, also called cyber crime, is any illegal activity arising from one or more Internet components, such as Web sites, chat rooms, or e-mail. Cyber crime can include everything from nondelivery of goods or services and computer intrusions (hacking) to intellectual property rights abuses, economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of other Internet-facilitated offenses.

Crime Moves Online

The IC3 began as a concept in 1998 with an appropriate recognition that crime was moving to the Internet because business was moving to the Internet, and the FBI wanted to be able to track that activity and develop investigative techniques specific to Internet crimes.

At that time there was no single place where people could report Internet-related crimes, and the Federal Bureau of Investigation (FBI) wanted to distinguish online crime from other criminal acts that are normally reported to local police, the FBI and other federal law enforcement agencies, the Federal Trade Commission, the U.S. Postal Inspection Service (USPIS—the law enforcement arm of the U.S. Postal Service), and others.

The first office, set up in 1999 in Morgantown, West Virginia, was called the Internet Fraud Complaint Center. It was a partnership between the FBI and the National White Collar Crime Center, a nonprofit contractor to the U.S. Department of Justice whose primary mission is to improve the ability of state and local law enforcement officers to identify and respond to economic and cyber crime.

In 2002, to clarify the scope of cyber crime being analyzed, from simple fraud to the range of criminal activities that were appearing online, the center was renamed the Internet Crime Complaint Center and the FBI invited other federal agencies—USPIS, the Federal Trade Commission, the Secret Service, and others—to help staff the center and contribute to the work on cyber crime.

Today at the IC3 in Fairmont, West Virginia, six federal agents and approximately 40 analysts from industry and academia receive Internet-related criminal complaints from the public, then research, develop, and refer the complaints to federal, state, local, and international law enforcement or regulatory agencies and multiagency task forces for investigation.

Through an IC3 Web site [*http://www.ic3.gov*], people from all over the world can file complaints about Internet crime. The Web site asks for a person's name, mailing address, and telephone number; the name, address, telephone number, and Web address, if available, of the individual or organization suspected of criminal activity; details about how, why, and when a person believes a crime was committed; and any other information that supports the complaint.

Building a Case

The main operational goal of the IC3 is to take an individual citizen's complaint that might represent a crime involving damages of, for example, $100, and combine it with information from 100 or 1,000 other victims around the world who have lost money in the same scenario, and build that into a substantial case as quickly as possible.

The reality is that most law enforcement agencies are not allowed to work cases that represent relatively small amounts of money—$100 is probably below the investigative threshold. But most bad guys are online to expand the scope of their victimization and moneymaking opportunities; a cyber crime almost never involves just one victim. So if IC3 investigators can link related complaints and turn them into a $10,000 or $100,000 case with 100 or 1,000 victims, then the crime becomes a more significant matter and law enforcement agencies will be able to investigate it.

IC3 sometimes helps law enforcement agencies by researching and building the initial case. In the first two and a half years of the project, despite an effort to build cases and refer them quickly to law enforcement agencies, IC3 investigators found that not all cyber crime task forces are equipped to quickly follow or investigate Internet-related crimes. Some task forces may not have the ability to do an undercover operation or the equipment to follow the digital trail of evidence the IC3 passes on to them, so it's increasingly important for IC3 to develop and follow the trail and build the initial case.

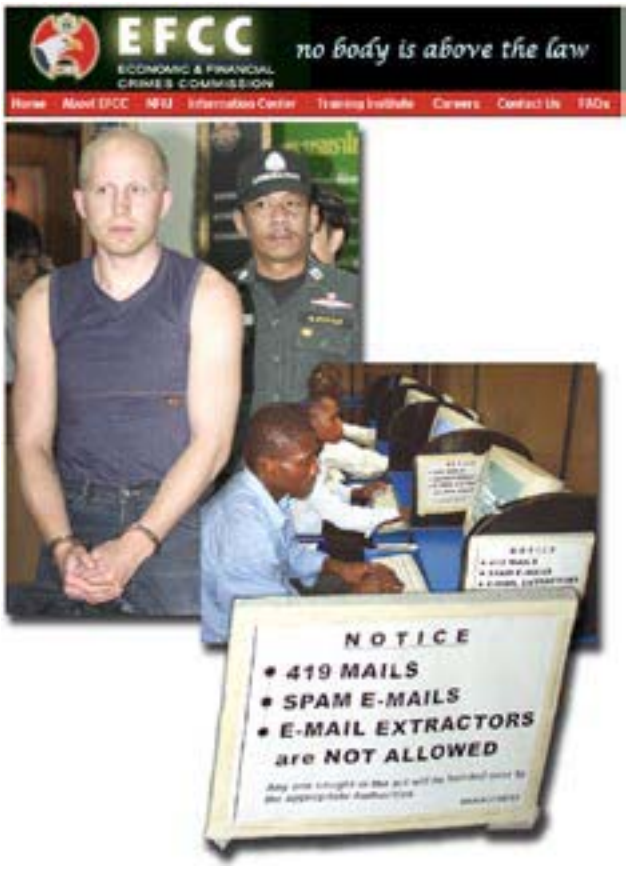
For example, the IC3 might identify 100 victims and determine that the criminal activity seems to be coming from a server in Canada, but actually that server is just a compromised machine. The bad guys are using it as a "bounce point" to mask their real location. So it is useful for IC3 analysts to learn more about the bounce point. It might be that a group in Texas, West Africa, or Romania is using the server in Canada to collect victim information.

Industry Alliances

Because IC3 analysts have found that it is better in some complex technical cases to follow the early investigative trail, the center created a spin-off for that purpose in Pittsburgh, Pennsylvania, called the Cyber Initiative and Resource Fusion Unit (CIRFU). CIRFU analysts eliminate false leads and refine a case before it is referred to a local or international law enforcement agency or task force.

CIRFU is supported by some of the biggest targets of cyber criminals—online organizations and merchants like Microsoft, eBay/PayPal, and America Online, and industry trade associations like the Business Software Alliance, the Direct Marketing Association, the Merchant Risk Council, the Financial Services Industry, and others. Investigators and analysts from these organizations, many of whom are already working on cyber crime issues, have joined CIRFU to identify Internet crime trends and technologies, develop significant cases, and help law enforcement agencies worldwide identify and combat Internet crimes.

At the CIRFU, federal agents and analysts from industry and academia work together to find out where the crime originates, who is behind it, and how to fight it. When the CIRFU hears from an industry group about a specific trend or problem, the unit forms an initiative to target some of the top offenders and make arrests, and not only prosecute them but learn more about how they operate. Then IC3 informs the public about the trends and scams through a public service advisory or alert that is posted on the IC3 Web site or disseminated in other ways.



Based on consumer complaints and industry data, the investigators monitor trends and problems and form six- to 12-month initiatives with industry partners to target specific criminal activities, including the following:

• **Reshipping:** An operation in which conspirators or unwitting accomplices in the United States are hired to receive packages of electronic or other merchandise bought with fraudulent or stolen credit cards, then repackage the merchandise for shipment, usually abroad. By the time the merchant finds out that the credit card was fraudulent, the merchandise is already in another country.

• **Criminal spam:** Unsolicited bulk e-mail that is used to commit financial institution fraud, credit card fraud, identity theft, and other crimes. Spam can also act as a vehicle for accessing computers and servers without authorization and transmitting viruses and invasive software to other computers.

• **Phishing:** Attempts to steal passwords and financial information by posing as a trustworthy person or business in a seemingly official (spoofed) electronic communication, such as an e-mail or a Web site.

• **Identity theft:** The result of an offender using someone's stolen personal information to commit fraud or other crimes. One bit of personal information is all someone needs to steal an identity.

International Outreach

The IC3 also works with international organizations, such as the Economic and Financial Crimes Commission (EFCC) in Nigeria, where a high level of economic and financial crimes like money laundering and the advance-fee fraud, or 419, have had severe negative consequences for the country.

Named for the violation of Section 419 of the Nigerian Criminal Code, the 419 scam combines the threat of impersonation fraud with a variation of an advance-fee scheme. A potential victim receives a letter, e-mail, or fax from people posing as Nigerian or foreign government officials, asking for help in placing large sums of money in overseas bank accounts, and offering a share of the money in return. The scheme relies on convincing a willing victim to send money to the letter's author in several installments for a variety of reasons.

Photo montage: The Internet Crime Complaint Center and other U.S. agencies work with international organizations like the Economic and Financial Crimes Commission (EFCC) of Nigeria and with law enforcement officials in other countries to combat Internet fraud. (Photographs from AP/Wide World Photos; Web banner courtesy EFCC)

In Nigeria, the menace of such crimes led to the establishment of the EFCC. Over the past year and a half, IC3 has made many new merchandise seizures and arrests in West Africa as a result of this and other alliances.

IC3 also works closely with the Canadian organization, Reporting Economic Crime On Line (RECOL). RECOL is administered by the National White Collar Crime Center of Canada and supported by the Royal Canadian Mounted Police and other agencies. RECOL involves an integrated partnership between international, federal, and provincial law enforcement agencies, and regulators and private commercial organizations that have a legitimate investigative interest in receiving economic crime complaints.

A growing group of international agencies are involved in fighting cyber crime. The IC3 works with law enforcement officials in many countries, including Australia and the United Kingdom. IC3 representatives also attend periodic meetings of the G8 (Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States) Subgroup on High-Tech Crime, part of which works to combat cyber crime and enhance cyber investigations.

The IC3 and the CIRFU projects are a constantly evolving work in progress. Along the way, IC3 agents and analysts revisit what is working and what is not working, and constantly seek out experts and sources of intelligence to get smarter about cyber crime and learn how to more effectively fight it. That is the constant charge at IC3. ■