Get hit by internet crime? Good luck getting help from some local police

March 13 2018, by Tim Johnson, Mcclatchy Washington Bureau

Credit: CC0 Public Domain

In practically the blink of an eye, Maggie Irizarry lost about $1,300 to thieves. But the culprits weren't robbers who broke into her Miami home. They were hackers who connived their way onto her Lenovo

laptop.

Because of that, local police balked at getting involved. Irizarry's only recourse was to plead for mercy with her bank and credit card company in hopes of recovering her loss.

Hundreds of thousands of Americas are victims of cybercrime every year. Yet only 15 percent of cyber fraud victims ever report the crimes to law enforcement, the FBI says. Many victims—those who have lost hundreds or thousands of dollars—feel they have nowhere to turn.

The truth is they often do not. Most local and state law enforcement agencies are not equipped to track down cyber crooks. The FBI is swamped and must prioritize big cases.

"It's a huge problem," said Nick Selby, a Texas police detective and information security consultant. "It's difficult for local law enforcement because we don't have the training."

International cyber gangs prey upon U.S. victims by hacking their computers to obtain credit card and Social Security numbers to defraud banks and retail outlets. But other crimes are also on the rise.

"They are things like, 'My ex is tracking me with spyware on my phone,' or 'My neighbor has hijacked my wireless and is doing illegal things.' There's nobody to tell about this," said Michael K. Hamilton, founder and president of Critical Informatics, an information security firm that operates out of Bremerton, Washington.

Local and state law enforcement agencies often are ill-equipped to investigate digital crimes, which can originate across state lines or outside of the United States. Prosecutors sometimes hesitate to take on complicated cases with low conviction rates. At the national level, a rise

in cases inundates the FBI, the lead federal agency on cyberattacks and crimes.

"This threat is now coming at us from all sides," FBI Director Christopher Wray said March 7 at Boston College. "We're worried—at the FBI and with our partners—about a wider range of threat actors, from multinational cyber syndicates and insider threats to hacktivists. And we're concerned about a wider gamut of methods."

For Irizarry, a chemical engineer who worked at the Environmental Protection Agency before her retirement, the threat came one day when her laptop screen turned bright red.

"It gave me a message to call Microsoft. Dumb me, I supposedly call 'Microsoft.' It was an 800 number," Irizarry said. "I panicked a bit."

The call responder said he would fix Irizarry's computer for $300, so she turned over her credit card number and gave the man remote electronic access to her hard drive.

Later, her phone rang. The callers said they'd overcharged her credit card by $1,000.

"They started screaming at me, saying they were going to be fired because they made this huge mistake," she said. Then they asked her to go to a CVS drugstore "and get $1,000 in gift cards in $100 denominations," she said. "At that point, I figured out that they were not Microsoft."

At the urging of a friend, Irizarry called the FBI, and an agent told her to alert her bank and credit card company. Then she went to city police.

"The guy said, 'I cannot take your complaint.' I said, 'Why not?' 'Because

you don't know who did this,'" she said. She said the man had an Indian accent, and the officer surmised that the internet scam operated from India.

"They do this all the time, he said, and we don't have jurisdiction over this. You don't have a name or an address," Irizarry recalled.

Luckily, the bank reimbursed her $1,000 loss and so did the credit card company. She held $500 in Apple gift cards that she had bought but not yet turned over to the fraudsters.

At the urging of the FBI, Irizarry filed an electronic complaint with the bureau's Internet Crime Complaint Center, a national clearinghouse. The center received 298,728 complaints with total losses in excess of $1.3 billion in 2016, the latest year for which statistics are available.

While the FBI sorts through and bundles even the smallest internet crimes, active investigations concentrate only when losses are large.

"We talked to one of the bigger field offices in the U.S. and they said, 'We have a million-dollar threshold.' There's just too much cybercrime for them to look at anything below $1 million," James A. Lewis, head of the technology policy program at the Center for Strategic & International Studies, said at a Feb. 21 event.

In a follow-up interview last week, Lewis said local police departments often have only one or two cyber specialists, and prosecutors and judges may not have significant expertise.

"There's a reluctance, I think, below the federal level to take on what can be very tough cases," Lewis said.

Selby, the Texas detective, said local police departments will take a

strong interest if a cyber case involves terrorism, human trafficking or child pornography.

"If you got your identity stolen and you're looking for more than a police report, no, you're out of luck," Selby said, adding that the matter is partly generational. "You still have generations of chiefs of police who are in their 60s. They are not really focused on this."

Some smaller departments have hired experts with formidable cyber forensics skills.

"There have been cases where I've been able to trace activity back to Eastern Europe," said Anthony Kava, a digital forensics examiner and special deputy at the Pottawattamie County Sheriff's Office in western Iowa. But FBI support is hard to obtain.

"There's a long queue to get things done because everyone wants their (the FBI's) assistance," Kava said.

At the Miami-Dade County Police Department, which is separate from the Miami City Police that declined to handle Irizarry's matter, officers are instructed to take all cyber complaints, said Sgt. Armando Borrego of the Organized Fraud Intelligence Squad. But cybercrimes that originate abroad are problematic.

"What recourse do we have? Our jurisdiction is Miami-Dade County. How do we put somebody behind the computer? Honestly, we can't," Borrego said.

Even the FBI struggles with getting hit by cybercrime.

Last month, the FBI alerted citizens to beware of criminals sending emails impersonating its Internet Crime Complaint Center, suggesting to

victims that they could receive restitution if they provided more information about themselves. The bogus emails contained an attachment.

"The text file contained malware which was designed to further victimize the recipient," an FBI release said.