The New York Times

October 24, 2004

Identity Theft Is Epidemic. Can It Be Stopped?

By TIMOTHY L. O'BRIEN

PAUSING in the foyer of a comfortable suburban home two days before Halloween in 2002, Kevin Barrows, a special agent with the F.B.I., could not bring himself to open the front door. He and a team of agents had just spent several hours searching every room in the house, in New Rochelle, N.Y., but they were leaving empty-handed. Months of investigating had led Mr. Barrows to believe that someone was orchestrating a huge fraud from the house, yet he had not found a single scrap of evidence.

Still, something bothered him about the furniture in one of the bedrooms. It seemed oddly oversized. So he headed back upstairs for a second look, and his attention focused on an expansive canopy over the bed. When he pushed at the draping, he found that it was weighed down with files. They contained reams of confidential financial information about hundreds of individuals whose identities had been pilfered in an intricate scheme that illicitly netted more than $50 million.

Two years later, the New Rochelle home has emerged as a linchpin in what federal law enforcement authorities describe as the biggest case of identity theft ever uncovered in the United States. The scheme was essentially masterminded by just two people: Linus Baptiste, who lived in the house and had contacts with a sprawling ring of Nigerian street criminals, and Philip A. Cummings, his former brother-in-law, who worked as a help-desk clerk at a Long Island software company. At least 30,000 people nationwide were victimized, according to law enforcement authorities and court documents.

"In a lot of ways it could have been the perfect crime," Mr. Barrows, who now works as a private investigator, recalled in a recent interview. "The execution was seamless, and if they had been smart enough not to use a phone line that traced back to that house we probably never would have found them."

The Baptiste case and others like it are at the forefront of one of the fastest-growing white-collar crimes in the country. Identity theft involves the most intimate, the most stealthy and perhaps the most intrusive of frauds - the wholesale lifting of someone's financial persona to secure bank loans, credit cards and mortgages in that person's name. Even when the crimes are discovered early, it can take months, sometimes years, for innocent people to restore tattered credit histories. While most consumers usually do not have to pay for illicit purchases on their credit cards, they may be held liable in thefts involving other types of loans.

"Ultimately, victims don't have to pay debts incurred by another person, but that's not the point," said Bridget J. Thomas, a homemaker in Prairieville, La., who spent months repairing her credit history in 2002 after a thief appropriated her identity to snare about $65,000 in loans. "It's the sleepless nights, and the time, and the stress you have to go through to clean up your record that really hurts victims."

ANALYSTS say several factors have combined to make identity theft a particularly intractable crime:

Exhibit C

the growth of the Internet and digital finance, decades of expanding consumer credit worldwide, the hodgepodge nature of local and federal law enforcement, and the changing but often still inadequate regulations governing the credit industry.

Everyone is fair game. Thieves recently snatched the identity of a three-week-old infant in Bothell, Wash. And authorities say that the dead have been favorite targets of identity thieves for years. Nor is identity theft limited to people. A growing number of thieves now assume the false guise of entire companies, adopting a business's employer identification number to secure commercial loans, corporate leases or expensive office products, according to analysts, security specialists and law enforcement officials.

Schemes known as "phishing" use e-mail messages to lure unwitting consumers to Web sites masquerading as home pages of trusted banks and credit card issuers, corporate security specialists say. Online visitors are then induced to reveal passwords as well as bank account, Social Security and credit card numbers.

The F.B.I. says that many identity thefts and cyberschemes that play out in the United States are hatched in Russia, Romania and West Africa and that the agency is trying to work with law enforcement officials in those places to stem the problem. A leading bank regulator, the Federal Deposit Insurance Corporation, warned in June that increased corporate outsourcing of call-center tasks and other jobs overseas had heightened the risk of identity theft.

Authorities have only recently grasped the full scope of the problem. It began to gain more attention a decade ago, prompting Congress in 1998 to make identity theft a federal crime and the Federal Trade Commission to set up a special victim assistance center a year later. Until a couple of years ago, analysts and federal authorities estimated the annual number of identity thefts to be in the hundreds of thousands. But in September 2003, the F.T.C. offered an eye-opening assessment of how widespread and damaging such crime might be.

In a report prepared by its consumer protection bureau, the F.T.C. said 27.3 million Americans had their identities stolen from April 1998 to April 2003 - with more than a third of them, or 9.9 million, victimized in the last 12 months of that period alone. The crimes ranged from the theft of a credit card number to more elaborate identity thefts used to secure loans. During those 12 months, the report said, businesses and financial institutions suffered about $48 billion in losses because of identity theft, and victimized consumers paid more than $5 billion in out-of-pocket expenses to regain their financial identities.

"The number of victims we were estimating in 2000 were 400,000 to 500,000 annually and by 2003 we were saying 750,000," said Linda Foley, executive director of the Identity Theft Resource Center, a nonprofit consumer advocacy group based in San Diego. "The business community said 'Oh, you are wrong; those numbers are wrong.' Well, we were wrong. The numbers were much higher."

Experts say identity theft has evolved from isolated examples, like Ms. Thomas's, to ever broader and more financially damaging cases, like the one investigated by Mr. Barrows, that involve the speedy theft and aggregation of hundreds or even thousands of identities. Many of the most vicious cases, say analysts, involve corporate insiders who hijack sensitive personal information from corporate databases in order to begin picking people's pockets.

"We're in the information database age, and insider theft has turned toward the theft of information, and specifically personal information, because with an assumed identity criminals can purchase goods and

services at will using someone else's credit," said Judith Collins, an associate professor of criminal justice at Michigan State University and an expert on identity theft. "Increasingly, we're seeing cases where identities are stolen in the U.S. and then used elsewhere overseas."

Last year, Dr. Collins completed a study of more than 1,000 identity theft cases from 1999 to 2002, the results of which she plans to publish soon. She said the report would indicate that about 5 percent of the crimes examined were linked to known or suspected terrorists.

Law enforcement officials say they believe that members of the Irish Republican Army and terrorists involved in the foiled plot to bomb Los Angeles International Airport relied heavily on identity theft schemes to finance their operations. Operation Web Snare, a Justice Department investigation of cybercrimes that was begun last summer, found possible links between identity theft and terrorism financing, according to a government report on the investigation.

Dr. Collins said her study would highlight other important aspects of identity theft. For example, the study will show that corporate insiders set in motion about half of the identity theft cases examined. The F.T.C. has reached similar conclusions.

"Insiders are often targeted or corrupted by organized crime groups to provide information," said Joanna Crane, manager of the F.T.C.'s identity theft program. "You might see groups plant someone at a temp agency or janitorial agencies so they can steal files when they are contracted out to work for someone else."

Or, as the partnership of Mr. Baptiste and Mr. Cummings showed, cultivating a corrupt insider may be simply a family affair.

Mr. Burrows, the F.B.I. agent, said he had his first inkling of the scheme in early 2002, after the F.B.I. office in Detroit passed along a fraud case to his New York supervisors that the Detroit agents believed was unsolvable. A former lawyer and Wall Street analyst, Mr. Barrows had successfully investigated securities fraud, and his supervisors tapped him to investigate the matter. At the time, the authorities knew that about 15,000 people had been victimized, largely because someone had used corporate codes and passwords to access their credit histories from reporting agencies like Experian, Equifax and TransUnion.

"It didn't take a rocket scientist to discover that the weak link was somebody who had stolen confidential subscriber codes and passwords," Mr. Barrows said. "But the question of 'who' was much more difficult to answer."

Mr. Barrows joined forces with an assistant United States attorney in Manhattan. The pair began to focus on who would be in a position to get the codes. Several companies across the country, all of which were unaware of the problem, had had their codes stolen. The companies were diverse - including banks, auto dealerships and a hospital - but each used a software product made by a Long Island company, Teledata Communications of Hauppaugue. The software allowed companies to use personal computers to request and download credit histories from reporting agencies.

Mr. Barrows focused on Teledata employees as likely perpetrators. He looked almost exclusively at the company's help-desk representatives, knowing that those employees interacted with customers who provided confidential personal information like Social Security numbers. Mr. Barrows and an Equifax employee also began cross-referencing Teledata's telephone records with Equifax records to find instances when small auto dealerships ordered unusually large batches of credit histories. He said that

phase of the investigation lasted four months and involved painstaking research akin to "looking for a needle in a haystack."

Luckily, Mr. Barrows and his Equifax colleague found their needle: a telephone number linked to Mr. Baptiste's home in New Rochelle.

AFTER Mr. Barrows discovered the credit files in the bedroom, he found a ledger detailing amounts paid and owed to Mr. Baptiste. Mr. Barrows also discovered a laptop computer hidden in the bedroom. It contained a document bearing the name of Mr. Baptiste's former brother-in-law, Mr. Cummings, who worked on Teledata's help desk.

According to court records and law enforcement officials, Mr. Baptiste approached Mr. Cummings in 2000 and offered to bribe him to download as many credit histories as possible, using appropriated corporate passwords and the Teledata software; at least 20 Nigerians in the Bronx and Brooklyn who were linked to Mr. Baptiste paid the pair $60 for each credit report acquired.

The Nigerians used the information to get credit cards in victims' names, the officials say. With the cards in hand, they went on shopping sprees at retail outlets like Home Depot, reselling their merchandise for cash to fencers for about half the purchase price charged to the cards. The identity thieves also used the pilfered information to deplete victims' bank accounts, change addresses on the accounts and take out loans.

All told, the Baptiste-Cummings ring stole identities from at least 30,000 people from 2000 to 2002, ringing up tens of millions of dollars in profits, according to law enforcement officials and court papers. While court papers describe Mr. Baptiste and Mr. Cummings as architects of the scheme, the United States attorney's office declined to comment on how the ring actually divided its loot.

Mr. Baptiste, Mr. Cummings and at least five other people were arrested shortly after Mr. Barrows searched the New Rochelle home. Mr. Baptiste and Mr. Cummings have pleaded guilty to fraud charges filed in federal court in Manhattan and await sentencing early next year. Their lawyers declined to comment on the charges, but Mr. Cummings, who appeared in federal court last month with an oxygen tube in his nose, is seeking a reduced sentence because he says his health is fragile. The United States attorney's office in Manhattan would not comment on whether other arrests were imminent.

"What everyone was horrified about in this case was how much damage could be done by one guy being in the right place at the right time," said Marcus Asner, one of the assistant United States attorneys prosecuting the Baptiste case.

William Nass, Teledata's president, said his company had screened Mr. Cummings carefully before hiring him and that his previous work record had included seven years at a major bank. Mr. Nass noted that Mr. Cummings worked for Teledata for just nine months beginning in June 1999 and that most of the crimes occurred after he left the company. While Teledata has since upgraded its products and procedures to defend against similar problems, Mr. Nass said that any company is vulnerable to crafty insiders.

Mr. Barrows agreed. "The hardest thing to battle is the insider because no matter what you do to try and prevent it, a corrupt insider will derail that," he said. He added that his case against Mr. Cummings and Mr. Baptiste "could really have gone unsolved except for fortuitous circumstances."

The fact that luck played such an important role in catching Mr. Cummings and Mr. Baptiste bothers

critics of corporate and law enforcement efforts to battle identity theft. While they laud ambitious investigations and prosecutions like the Baptiste case, they note that such cases are rare.

"One of the key major problems is that prosecutors do not want to take on identity theft cases because they're so hard to prosecute," said Dr. Collins at Michigan State. "We're burdened with an elephant of a law enforcement bureaucracy nationwide that makes it difficult to prevent or even mitigate identity theft."

President Bush recently signed into law tougher punishments for identity theft, but some law enforcement officials say that hurdles remain. They say that smaller cases are sometimes ignored or delayed until they can be bundled into high-profile, high-impact prosecutions. "It's the simple reality of us trying to build that small case into something larger before I commit resources to it," said Dan Larkin, head of the F.B.I.'s Internet Crime Complaint Center. "For me to try to build that case I'm going to need to ratchet it up a little bit."

Mr. Larkin said that the F.B.I. has been pushing for the last few years for greater cooperation among the bureau and state and local law enforcement agencies, and that the F.B.I. now had an "excellent ability to plug into" local identity theft investigations when invited.

For many victims, securing a police report can be an onerous, sometimes endless process. Local police departments often do not issue reports for residents if the identity theft occurred elsewhere, and most states do not require the police to do so. Yet credit issuers and reporting agencies typically demand a police report before they take a victim's claims seriously, often leaving consumers at a loss when they try to repair sullied credit histories.

Last year, President Bush signed a law that expands consumer credit protections and also offers provisions making it simpler for consumers to resolve identity theft problems and protect their accounts. The new law, which does not take effect until Dec. 1, also aims to make it easier for consumers to get police reports when their identities have been stolen.

A survey released last year by Gartner Inc., a research firm specializing in information and technology issues, criticized banks, financial service firms and other pillars of the credit industry as not putting into effect more rigorous computer screening procedures to protect customer accounts. It also said that ineffective screening ultimately forced identity theft victims to bear most of the crime's social and economic costs.

"We've created a victim population that is self-blaming," said Ms. Foley of the Identity Theft Resource Center. "Most of these problems start with companies that are too loose with consumer and employee information."

Some victims, after enduring the slow torture of mending their credit histories, say they know exactly whom to blame. "My anger at my perpetrator quickly transferred to the credit-granting community itself," said Ms. Thomas, describing how her emotions shifted after her creditors largely ignored her efforts to overcome identity theft. "They don't care what this does to victims because they don't have to care."

BANKS and others in the credit industry disagree, saying that they see the war on identity theft as a top priority. Nessa Feddis, senior federal counsel at the American Bankers Association, says fraudulent credit card charges, have been declining as a percentage of overall charges. Ms. Feddis, who was able to resolve her own past identity theft problems by placing a call to the Secret Service, says banks are

"doing a good job of educating their customers" about identity theft and "providing ways to assist them."

A spokesman for the Consumer Data Industry Association, the trade group representing credit reporting agencies, said consumers could put fraud alerts on their credit histories if they wanted to keep prying eyes at bay. Representatives of Visa and MasterCard, the two largest credit card associations in the country, say that they are guarding customer account numbers more carefully, for example, by deleting the numbers in mail and other documents delivered to customers' homes.

Sergio Pinon, the head of security and risk services at MasterCard, said that MasterCard was deploying computer systems that analyze the spending patterns of individual card users and pluck out anomalies in case a fraud is under way. Like Ms. Feddis, Mr. Pinon said that he was the victim of an identity thief, but that he stopped the fraud because his bank had quickly spotted an intrusion into his credit card account.

Both MasterCard and Visa also monitor Web sites that broker stolen credit card numbers and other personal information. "One of the things we've discovered is that your identity is worth about $10" on the Internet, said Linda Locke, a MasterCard spokeswoman.

With identities so cheap, experts say that criminals who want to mask themselves inside the envelope of someone else's financial world will continue to have ample opportunities to express themselves.

"The only limitation to identity theft is the creativity of the thief, and that's scary because there's really no limit on creativity, is there?" Ms. Foley said. "The tour guides on this crazy ride are the thieves, not us and not law enforcement, and as long as that continues it's going to be a problem."