PLAINTIFFS' ATTORNEY ANNE SIMON
An atmosphere poisoned.

protested" from 1973 until her graduation this spring. As a result, she claimed she "found it impossible to continue playing the flute and abandoned her study of the instrument, thus aborting her desired professional career." Another plaintiff, a 19-year-old junior, alleged she was subjected to repeated "sexual harassment" this spring every time she visited an English professor's office to discuss term papers. Anne Simon, a Yale Law School alumna who is representing the plaintiffs, estimates that 75 such incidents occur at Yale every semester.

Jose Cabranes, Yale's attorney, denounced the suit as "reckless and obviously designed to attract maximum publicity for groundless charges." He said the university already had a system for investigating the harassment of students —but it is a system set up last year only to aid blacks, and has never been used to investigate sexual coercion charges.

Computer Capers

Many nights after most employees had gone home, the main computer at Sperry Univac's office near Philadelphia continued to hum. Two programming supervisors, David E. Kelly and Matthew Palmer Jr., had taught the machine to store and print complicated arrangements for musical groups, which the two then peddled to stores and bands. In the course of three years, the entrepreneurs bilked Sperry Univac out of some $144,000 in computer time. And they might never have been caught if another employee had not informed on them.

The incident was a new twist in one of the fastest-growing industries in the U.S.: computer crime. It has grown from nothing 20 years ago to a 3,000 million annual racket today. With financial transfers increasingly taken over by electronic data-processing (E.D.P.) systems, the prospects for future swindles appear limitless. Says Philadelphia FBI Agent Michael Boyle: "This is the crime of the future."

Only one of every 100 computer ripoffs is ever detected, according to an industry expert, although some reported frauds have been enormous. The biggest to date was the $2 billion Equity Funding scandal of 1973, in which 22 insurance company employees were convicted of inventing some 56,000 fake policies for resale to other insurance companies. Other binary burglars programmed Penn Central computers to divert 237 freight cars to an obscure Illinois railroad siding, where both cargo and cars were plundered. An electronics expert aged 19 gained access to Pacific Telephone & Telegraph terminals and managed to order $1 million worth of supplies over nearly two years.

Traditional auditing methods are powerless to stop sophisticated E.D.P. swindlers because accountants no longer can reconstruct a "paper trail" of records; a clever programmer can order the computer to erase all traces of his own incursion. Admits FBI Computer Expert James Barko: "Many cases are discovered completely by accident," like noticing suspicious high living by low-paid clerks. After raiding a New York bookie, police traced a $30,000-per-day betting account back to an $11,000-a-year teller at the Union Dime Savings Bank and discovered that he had made off with $1.3 million by the computerized shuffling of funds among little-used accounts. Even if caught, a computer thief may not be prosecuted. Fearing embarrassing publicity, some firms merely fire the offender and absorb the losses.

Cracked Open. Now the FBI has started a special computer-fraud program at its training center in Quantico, Va. Instructors have set up a model computer-controlled bank, complete with fictional account holders and loan applications, and they give the students only a few clues about what kinds of fraud might be involved. Next month the FBI school will begin giving its four-week training course to state and local policemen.

FBI agents trained in the Quantico center received the tip about the moonlighting music publishers in Philadelphia and cracked the case wide open. But their efforts may receive a setback this week, when U.S. Judge J. William Ditter rules on defense motions to throw out the indictments. The reason: no federal law specifically prohibits the theft of computer time or computer data. The U.S. Attorney decided to charge the pair with mail fraud for advertising their music, and that may prove inadequate.

Several other federal cases have nearly foundered because of insufficient laws. The conviction of one man, accused of stealing confidential information from a Federal Energy Administration computer in Maryland, was possible only because the thief had dialed into a system from his office a few miles away in Virginia. He was prosecuted under an interstate wire-fraud statute. In response, Senator Abraham Ribicoff has introduced a bill prohibiting misuse of federal computers or any data-processing machine affecting interstate commerce. The bill would impose stiff punishments: up to 15 years in prison and a $50,000 fine. Says Justice Department Prosecutor Tate De Wese: "This bill fills the gaps."

Neither draconian laws nor increased police action is likely to thwart computer thieves. Most authorities agree that computer owners must install more elaborate security measures. Says one: "Cracking a computer system's defenses is about as difficult as doing a hard Sunday crossword puzzle." One computer, protected by a five-digit code number, was illegally entered in minutes when the thief ordered the computer to begin trying every one of the 100,000 possible combinations. But tighter security would cost both money and time. Says Robert Courtney of I.B.M. "If you're running thousands of transactions a day, you don't want to spend ten seconds or so every time arguing with the computer about who you are." Some manufacturers are experimenting with personal passwords, such as fingerprints, voice prints and even lip prints that can turn on an E.D.P. machine. Inventors are trying complicated locks utilizing algorithmic principles. But even the most sophisticated security device cannot stop an unscrupulous employee with legitimate access to the machine and its workings. As one expert jokes, "Ideally, the first step in securing a system would be to shoot the programmer."

FBI'S BARKO WITH COMPUTER UNIT