

The Growing Threat of Identity Theft

Brian Ristuccia walked the fine line of ethical conduct in exposing a security flaw on the New York University (NYU) Web site. According to Ristuccia, in December 2003 he attempted to notify the university administration that it had inadvertently left students' personal information exposed. After receiving no response, he took that data—including Social Security numbers—and posted it on his own Web site. NYU then reported to 1,800 students that the security of their personal data had been compromised.

Ristuccia followed the pattern of many hackers who test their computer skills by looking for security flaws on the Internet, often on corporate or college and university Web sites. Acceptable practice within the hacker community allows for the public exposure of such flaws only after the organization at fault has been given the opportunity to respond by solving the problem. Whether Ristuccia acted honorably is subject to debate. He was among a minority who, in similar situations, have chosen to publicize the private information, but his easy access to the information was certainly not a unique situation. In recent months, students' private information held in college and university databases has been compromised and exposed time and again, a type of incident that is bound to increase as more information becomes digitized. For example, in January 2004, the University of Georgia discovered that hackers had broken into a server containing information about applicants for admission over the past few years; the data included Social Security numbers, birth dates, and credit card information. And in

2003, someone stole personal information regarding more than 50,000 current and former students, faculty members, and staff at the University of Texas at Austin.

Of more concern than the break-ins themselves is the ease with which hackers can use such information to steal the identities of members of the campus community. Identity theft is one of the fastest-growing crimes in the country, and those committing the crime often need little more than a name and a Social Security number.¹ Additional details, like date of birth, remove any barriers to the use of someone else's information. During 2003, the Federal Trade Commission (FTC) received nearly 215,000 reports of identity theft, up from 162,000 in the previous year. Identity theft represented 42 percent of all complaints received by the FTC, reflecting a growing trend.

Personally identifiable information, once stolen, can be used to apply for credit cards and benefits under the guise of another person's name. Not all identity theft is committed online; in fact, the easiest way to obtain such information remains going through the trash to look for bank statements, credit card offers, and receipts. But hackers who break into databases can steal thousands of sets of information at once, which they may use over the course of years. And once someone's credit has been ruined by a thief, a great deal of time and effort is generally needed to clear it. Doing so currently requires the involvement of law enforcement agencies, credit reporting bureaus, and the federal government.

Not all of the identity theft cases reported to the FTC in 2003 originated in

college or university communities, but identity theft is of growing concern in those areas because many academic institutions use Social Security numbers as student ID numbers. Students, many of whom are in charge of their finances for the first time in their lives, are also less likely to be aware of what information is acceptable to give out and are less likely to notice if that information has been misused.

In response to these problems, federal agencies have posted resources, some aimed specifically at campuses, for helping victims of identity theft. The U.S. Department of Education's identity theft Web site (<http://www.ed.gov/about/offices/list/oig/misused/idtheft.html>) focuses on educating students about the risks they face. It notes that nearly half of all college students receive credit card applications daily or weekly, most of which are thrown out without first being shredded; about one-third of students rarely reconcile credit card and checking account balances; and half of students have had grades posted by Social Security number.

To combat the problem on a legislative level, in 2003 Congress passed the Fair and Accurate Credit Transactions Act (FACT Act), a law designed to make it easier for individuals to clear their records after their identities have been stolen and harder for businesses to use personally identifiable information in insecure ways. The FACT Act, which became law on December 4, 2003, amended the Fair Credit Reporting Act "to enhance the ability of consumers to combat identity theft, to increase the accuracy of consumer reports, and to allow consumers to

exercise greater control regarding the type and amount of marketing solicitations they receive.”² In practice, it allows individuals to get free annual copies of their credit histories, creates a national fraud-detection system so that victims of identity theft do not have to notify each credit bureau separately, and requires businesses to hide Social Security numbers and portions of credit card numbers on receipts.

The act does not specifically address the use of personally identifiable information by academic institutions.



Common uses for Social Security numbers in such settings are as student ID numbers or as identifiers used by professors to match students to grades received in a class. As in the University of Texas case, institutions often do not store personally identifiable information separately from other data that could be used, in combination with this information, to steal a person’s identity.

On the state level, several legislatures have passed or are debating bills requiring that colleges and universities discontinue the use of Social Security numbers as student ID numbers. For example, while the University of Texas was embroiled in controversy surrounding its data-protection practices, the Texas State Legislature was considering such a measure. The bill, which remained in committee at the end of the legislative session, prohibited the use of four or more consecutive digits of a Social Security number as a student ID. It also would have

prevented institutions from using that number on ID cards or library cards, from requiring that students transmit Social Security numbers by telephone or Internet without encryption, from posting Social Security numbers in public places, and from using Social Security numbers in information mailed to students.³

The Florida State Legislature is currently debating a similar bill. States that have already passed laws prohibiting or limiting the use of Social Security numbers as student identifiers include New York, Washington, Arizona, and California. The California law, passed in September 2003, was part of an extensive bill aimed at combating identity theft in both the commercial and the public sectors. On a staggered schedule between 2004 and 2007, California universities, colleges, and community colleges, as well as the California Student Aid Commission, will be required to limit the use of Social Security numbers as student identifiers.

Institutions that have been hit with hacking or data-theft incidents have responded in various ways. Many have posted reports about the incidents on their Web sites, sometimes outlining how they are working to prevent similar breaches in the future. Georgia Tech—which had its event ticket-ordering database broken into in 2003, resulting in the theft of names, addresses, and credit card numbers—passed along information about the incident to the credit bureaus and law enforcement authorities. Administrators also removed the server in question from the network so that no further data could be taken.

By and large, colleges and universities are unable to determine whether stolen information will ever be misused. The incident at NYU was unique because the perpetrator publicized the fact that he had obtained personal information and because he attached his name to the act. In most cases, the only thing that academic institutions can do is warn students to keep an eye out for suspicious activity on their credit card or bank account statements. Sites put up in re-

sponse to a security incident often include resources for students who may have had their identities stolen, including contact information for the major credit bureaus. The FTC, like the Department of Education, also has on its Web site (<http://www.consumer.gov/idtheft/>) detailed information about how to deal with identity-theft incidents.

NYU handled its incident by notifying students whose information had been compromised, but just one month later, a student discovered that personal data about another 2,000 students, faculty, and staff members was publicly available in a different context. It was only after this second incident that the administration started to take a closer look at several campus Web sites to see how they protected private data. One additional site was found to have security issues and was shut down.⁴

Although it is virtually impossible for administrators to keep track of the specific information on every Web page that is part of a college or university network, they can combat identity theft by educating students to watch out for it and by implementing proper security on the network. The number of cases of identity theft reported to the federal government has been doubling every year. The problem will not go away on its own.

Notes

1. For additional information and resources, see the Identity Theft Current Issues page on the EDUCAUSE Web site: <<http://www.educause.edu/issues/issue.asp?ISSUE=IDTHFT>>.
2. See Federal Reserve System and Federal Trade Commission, “Effective Dates for the Fair and Accurate Credit Transactions Act of 2003,” <www.federalreserve.gov/boarddocs/press/bcreg/2003/20031216/attachment2.pdf> (accessed April 27, 2004).
3. Texas HB 1026, Legislative Session 78(R), “An act relating to regulating the use of social security numbers by institutions of higher education,” sponsored by Hupp, Rodriguez, Dukes, Miller, Naishtat et al., <<http://www.capitol.state.tx.us/tlo/78R/billtext/HB01026E.HTM>> (accessed April 27, 2004).
4. Andrea L. Foster, “New York U. Reports Another Lapse in Web Security,” *Chronicle of Higher Education*, February 20, 2004.

Elizabeth Goldman is a master’s student at the University of Michigan School of Information. She recently completed an internship with the EDUCAUSE policy team in Washington, D.C.

