

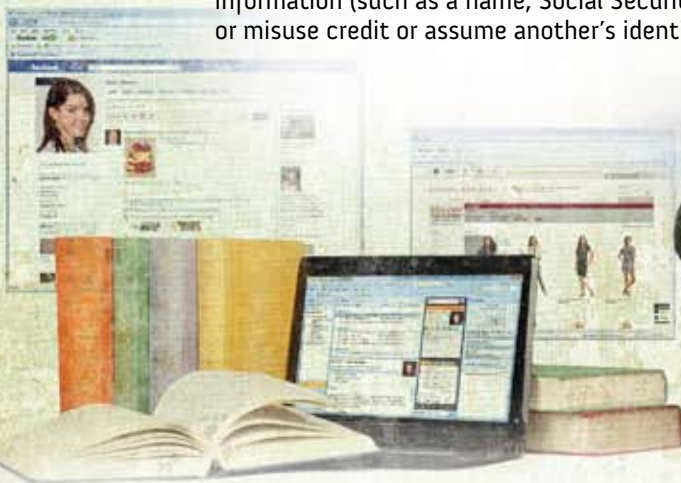
Fraud in the Quad

Campus life puts students at risk for identity theft

It's a typical day for Bethany, a freshman in college: She wakes up, chats with her roommate and opens her laptop to print a paper. Before heading to class, she stops at the cafeteria, where she leaves her backpack with friends while she gets something to eat.

After class, Bethany studies for an exam at the library. She leaves her laptop on a table while she speaks with a classmate. When she returns, she joins the library's wireless network to order some clothes online and update her blog and Facebook profile. Later, she heads back to her room, where a friend stops by with people Bethany has never met. They hang out, and then she steps out while her roommate's friends come and go.

Bethany goes to bed unaware that at many times that day she put herself at great risk for a serious crime: identity theft—the illegal use of someone else's personal information (such as a name, Social Security number, address or birth date) to establish or misuse credit or assume another's identity. [Continued on page 3](#) ▶



Credit Pirates Get Savvy

How sophisticated identity thieves hijack your credit security

In the past, an identity thief's repertoire included the basic account takeover. He would assume control over a victim's bank or credit card account to run up charges.

Now, criminals are getting savvier. They're using a victim's personal information to hijack entire credit reports and security protections. This means they can control all of a victim's accounts, open new accounts and remove any credit alerts or freezes warning creditors that an individual may be a victim of identity theft.

Identity Theft 911 calls these criminals "credit pirates" because they effectively take control, raising their flag over a victim's credit and extending the time period during which they can steal from that individual. [Continued on page 4](#) ▶



There should be a special ring in hell reserved for family members and friends who violate our trust, compromise our finances and commit crimes in our name. In this month's issue we examine the financial and emotional devastation wrought by frenemy and family fraud.

The college experience should be one of the most memorable periods in our lives—exposure to people from all walks of life, new places and exciting ideas that were only a far-off, potentially unattainable dream in our first 12 years of education. Unfortunately, the liberation of dorm life, rush week, wide-open Wi-Fi networks, all night study sessions, parties and floating from class to class can open the door for account compromise and identity theft. The mantra of “never let your studies get in the way of your education” could lead young people to a take walk on the dark side of life.

Roommates may arouse our suspicion, but relatives usually get a pass. That's when family fraud can strike. Ray Dunlap was devastated to learn that his father opened credit cards in his name and rang up \$30,000 in charges. With his financial life in limbo, will Ray turn in his own dad? Find out in our story on page 5.

We also introduce a new, frightening class of identity thief: credit pirates who obtain enough of a victim's personal information to hijack his credit report and security protections. These crooks target people with high credit scores and go through a lot of work to lengthen the amount of time they can steal from their victims.

Learn how Identity Theft 911 Fraud Specialist Maria Valenzuela is helping John Nathanson, a victim of child identity theft for the past 15 years. Someone who owes \$40,000 of back child support has been using Nathanson's Social Security number since Nathan was 7. Valenzuela is fighting to get Nathanson a new SSN.

Finally, be sure to check out our Hits & Misses, a roundup of the latest fraud-related news, as well as a Q&A with Vicki Volkert, a veteran fraud specialist who advises a victim on what to do after a cousin steals her identity.

As always, we hope you will enjoy.

Adam K. Levin
Chairman and Founder,
Identity Theft 911

In this issue...

Features



- 5 Family Fraud:** Ray Dunlap's father stole his identity. Years later, he's still dealing with the consequences. How to avoid identity theft when it's close to home.
- 6 Case Study:** John Nathanson may not get a student loan because his Social Security number was stolen 15 years ago. Learn from his experience with child identity theft.

Departments

- 7 Hits & Misses:** A roundup of who's getting it right and wrong in the fight against identity theft.
- 8 Ask the Expert:** Identity Theft 911 Fraud Specialist Vicki Volkert offers tips on what to do when a friend or relative steals your identity.

What made Bethany vulnerable? A few obvious things: She left her laptop out in plain view of strangers; she left her backpack, with her student ID and wallet, unattended; and she accessed password-protected accounts and used a credit card online through a wireless network. Bethany's day was rife with opportunities for an attentive thief, but her riskiest move was probably the one she would have least expected: She trusted her friends and acquaintances.

Identity theft strikes 11 million people per year, according to Javelin Strategy & Research. It is the crime most commonly reported to the Federal Trade Commission, which said that attacks

first car loan or mortgage, or even a job that requires a credit check.

It takes surprisingly little to set up a fraudulent account—sometimes just a Social Security number (SSN) and address will do. Bethany made available plenty of information about herself. Her computer was accessible to anyone in her room or at the library, and she put vital details about herself online.

“Don't put too much personal information out there,” said Vicki Volkert, an Identity Theft 911 fraud specialist. Students “tend to do that. With a little information from Facebook and another source, a thief can patch together enough information

shared space, knew so much about each other. Most college-age victims don't have that sense of awareness yet that something's not right. They're innocent,” she continued, “and they're surprised.”

By following some tips below, college students can brush up on the warning signs of and protect themselves from fraud, while still enjoying all that academic life has to offer. •

“Don't put too much personal information out there. With a little information from Facebook and another source, a thief can patch together enough information [to steal from you].”

— Vicki Volkert, Identity Theft 911 fraud specialist

against victims under the age of 19 represent 7 percent of all complaints. Fraudsters open credit cards, rent apartments and set up utility and cell phone accounts in victims' names, then skip out on the bills, leaving victims with drained accounts and damaged credit. Sadly, identity theft often is committed by someone who knows the victim—such as a roommate, colleague or family member.

College students make desirable victims for “frenemy fraud” or “familiar fraud.” They're trusting, quick to share information and possessions, and welcoming of new friends. They usually have very little credit history, don't check their credit reports or bank or credit card statements often, and don't notice a problem quickly, if at all. In some cases, the crime comes to light long after the victim has lost touch with the perpetrator—sometimes years after college, when the victim applies for his

[to steal from you]. Students have to be vigilant. They don't realize that giving out information—especially SSNs—may give fraudsters an opportunity.”

While the open, casual atmosphere of campus life is essential to the college experience—higher learning, after all, is about the exchange of ideas—it also makes students particularly vulnerable and promotes a false sense of security. Members of the school community aren't trustworthy just by virtue of their shared interest; thieves often use their commonality with the victim to instill trust, feigning friendship or romantic interest and gaining access to the victim's room, belongings and even passwords or account numbers.

Identity theft by a friend, acquaintance or roommate is difficult to accept. “Victims think they're friends [with the perpetrator] and feel betrayed,” Volkert said. “There's a lot of anger because they

Frenemy Fraud 101

1. Be wary of whom you befriend, especially people who ask a lot of questions or try to get to know you too fast.
2. Be alert. If a roommate starts buying expensive things—computers, new clothes—consider how he or she is paying for them.
3. Lock doors and drawers. Secure financial documents and personal information.
4. Don't reveal too much personal information—such as your birth date and hometown—in person or online.
5. Never share passwords, credit or ATM cards, or a checkbook with anyone else.
6. Never apply for credit cards at solicitation tables on campus—the applications and your information are not secure.
7. Don't use peer-to-peer software allowing computers to share music or any other files.
8. Password-protect computers, encrypt files, and lock up computers and paper files.
9. Buy a crosscut shredder. Make sure you use it on any paperwork with your name and other personal identifiable information.

“These crooks aren’t just Dumpster-diving or pickpocketing,” said Identity Theft 911 Fraud Specialist Mark Fulbright. “They’re adapting to new security technology and procedures to defraud people.”

How do they do it?

Credit pirates get the detailed information they need on prospective victims through major data breaches at financial institutions or medical organizations—banks, hospitals or even smaller outfits such as a doctor’s office or insurance agent’s business. The information can include some combination of names, addresses, birth dates, SSNs, all of an individual’s credit accounts and previous home addresses.

Breaches of this nature are increasingly more common. By early August, health-care organizations reported 119 significant breaches and financial services firms disclosed 39, according to the Identity Theft Resource Center, a San Diego-based nonprofit. Once a credit pirate gets hold of this data, he has enough information to

access a person’s credit report. He can answer the personal questions credit bureaus ask before granting access to the reports—especially details such as previous home addresses and a mother’s maiden name.

When the thief gains access to the credit report, he acquires even more information—enough to obtain almost any type of credit in the victim’s name. And even worse, he can then use that

warn creditors to verify a customer’s identity before issuing credit. He can undo security freezes, which block creditors from opening new accounts or granting credit. And he can approve all credit requests.

Credit piracy “is a lot of work, but it’s smart because the thief can continue committing fraud on an account for a longer period of time,” said Raul Vargas, a team leader in the Identity Theft 911

“These crooks aren’t just Dumpster-diving or pickpocketing. They’re adapting to new security technology and procedures to defraud people.”

— Mark Fulbright, Identity Theft 911 fraud specialist

information to render useless any identity-fraud security precautions.

Posing as the victim, the credit pirate can do just about anything to sustain access to the account: He can replace the victim’s contact information with his own. He can remove credit alerts, which

Fraud Resolution Center. “It’s easier for a thief to move from one victim to the next.”

In these cases, thieves target individuals with high credit scores so they can secure and use as much credit as possible.

There’s not much a victim can do except remain vigilant, checking daily to see if someone has applied for or received credit in his name, Fulbright said.

“It’s scary,” Fulbright said. Credit pirates “are showing everyone, ‘This is what I can do.’ They walk right through the front door of the credit bureau and do whatever they want.”

One partial solution for lawmakers to consider: Require credit bureaus to make their security measures and questions more detailed and sophisticated so that only the actual customer can gain access to his or her credit file. •

How to fight credit pirates

Follow these steps if you suspect a credit pirate has hijacked your credit report:

1. File a detailed report with local law enforcement.
2. Place a fraud alert on your credit file with any one of the three major credit bureaus. An alert signals to potential creditors that you may be a victim of identity theft.
3. Review your credit report thoroughly for any unusual activity.
4. Consider placing a security freeze on your credit report. A freeze locks access to your credit, so no one will be able to open a new account in your name. When you’re applying for credit, you can lift the freeze temporarily.
5. Contact existing creditors—your bank and credit card companies—to tell them you’ve been a victim of identity theft.

All in the Family

There's no easy answer when a relative steals your identity

Ray Dunlap* set off for college equipped with a Discover Card in his name, opened by his father. Dunlap used the card to buy a computer and other essentials with the understanding that his father would foot the bill.

Unfortunately, Dunlap's father also opened Visa and American Express cards in his son's name without telling him. He ran up \$30,000 in charges for goods including televisions, paintings and fine furniture. Now, more than a decade later, Dunlap is still saddled with debt, poor credit and a strained relationship with his father. Yet he balks at the idea of filing a police report against his perpetrator. "I can't send him to prison," he said. "He's still my father."

Dunlap's experience is common among victims of family fraud, a form of identity theft that's committed by a victim's relative. The crime is relatively easy to carry out since family members often share space, mailboxes and computers. They also share secrets and trust, which can make the crime tempting for perpetrators and devastating for victims.

The recession has made family fraud attractive for people who are in tough financial straits. Many cases that are being handled by the Identity Theft 911 fraud resolution center involve small sums, such as utility bills, rather than large purchases.

"Right now, when so many people have lost their homes, it's happening to more middle-class people," said Eduard Goodman, Identity Theft 911 chief privacy officer. "There is a constant level

of people doing it out of spite, but at times like this, we see people doing it out of need, just to keep the heat on, or the air conditioning."

Some 33 percent of medical identity theft victims said a relative stole their personal identification credentials without their knowledge, according to a recent study by Ponemon Institute, which researches privacy, data protection and security. Nearly half of medical identity theft victims said they knew the person who used their information.

"A family member will pose as someone else to get treatment or drugs," Goodman said. Or it's complicit: Someone will say, 'Take my medical card,' to help out a family member who has no insurance."

Because many victims of family fraud don't report the crime to the police—for fear of implicating a loved one—they often assume the financial consequences of the crime, in some cases paying off the debt slowly and enduring bad credit for years.

Financial institutions won't help unless a victim files a police report. But even if the money can be paid back (either by the impostor or by the victim) without involving the police, it's hard for relatives to forgive and forget.

The emotional fallout can be crippling for many victims. The breach of trust can break up families. In Dunlap's case, his father's reckless financial habits contributed to his parents' divorce. He and his brother are estranged from their father.

Dunlap said his father started out with good intentions that were overcome by his taste for the high life. Although Dunlap's credit score is improving over time, he said he wouldn't wish this experience on anyone.

"My story is not so much a cautionary tale to kids, but to parents," Dunlap said. "You may not know it, but you can really screw up your child's life if you do this." •

* Name and location have been changed to protect the victim's privacy.

Avoid theft close to home

1. Lock financial documents in a file cabinet and hide the key in a creative place.
2. Rent a secure mailbox and safe-deposit box if you don't trust a family member.
3. Change computer passwords to something they could never guess.
4. Shred early and often—especially credit card offers, pay stubs, utility bills and anything showing your Social Security number.
5. Check your credit report annually at annualcreditreport.com.



STUDENT LOAN APPLICATION

Child ID Theft:

Kids and teens are prime targets for identity thieves

John Nathanson* is preparing to attend Weber State University in Utah this fall. But he and his parents worry he won't qualify for a much-needed student loan.

Routine credit checks turn up \$40,000 in unpaid child support on his Social Security number (SSN). But Nathanson, 22, has no children.

For the past 15 years, an undocumented immigrant has used Nathanson's SSN for employment purposes. His parents discovered the problem in 1995, when the Internal Revenue Service told them they couldn't claim their son as a deduction on their tax return because his SSN was already in use. They took steps to correct the problem, but it persisted.

"It's been stressful," Nathanson's mother, Tanya, said of their ordeal. "It has taken hours and hours and hours of time."

When Nathanson was 16, he landed his first job. Everything was going well until a California county informed his new employer that he—or, rather, the man using his SSN—owed thousands of dollars in child support. When Nathanson was 19, the IRS took his \$380 tax refund to pay for the man's child support. Nathanson later received notices from the IRS saying he owed income taxes for jobs he never worked.

He has found it difficult to successfully apply for anything that requires a SSN—such as car insurance. Even communicating with the credit bureaus to monitor his credit has been a challenge because, he said, "They wouldn't talk to me because my name doesn't match my Social Security number."

The Nathanson family's homeowners' insurance included Identity Theft g11's services. His mother was referred to fraud specialist Maria Valenzuela, who immediately assessed the gravity of his case. The perpetrator had been using Nathanson's SSN for so long that it no longer registered as his; it registered as the perpetrator's.

"Most of the time we felt like nobody cared," Tanya said. "Having somebody else who has been acting as our agent has just been a relief. And Maria is trained on who to call and who to contact."

"Most of the time we felt like nobody cared. Having somebody else who has been acting as our agent has just been a relief. And Maria is trained on who to call and who to contact."

— Tanya Nathanson, mother of child identity theft victim

Valenzuela is working to secure a new SSN for Nathanson, a move the Social Security Administration only allows in dire circumstances. His situation fits the criteria for getting a new number. Nathanson hasn't been able to establish credit or even monitor his credit because his SSN is so strongly associated with the other man. Without a new number, Nathanson "would have to dispute information on his credit file for the rest of his life," Valenzuela said.

"I feel like we're at the end," Tanya said. "It's going to get fixed, and he can move on." •

* Names and location have been changed to protect the victim's privacy.

Hits



FTC to Advertisers: You Can't Track This

In response to concerns about online privacy, the Federal Trade Commission is considering a proposal for a national Do Not Track registry. Chairman Jon Leibowitz said the list would follow the same principles as the successful national Do Not Call registry. It would use an opt-out model for individuals to decline having their online activity tracked by advertisers. In a Senate hearing, Leibowitz said the agency also wants websites to make their most important privacy information clear and obvious, so regular Internet users "don't have to sell their soul for not opting out."



Kerry Bill to Protect Consumer Data

Senator John Kerry of Massachusetts said he plans to introduce an online privacy bill that he hopes will be passed in early 2011. The Kerry bill would establish rules to protect consumers from the improper collection and use of personal information in marketing, and set up guidelines for how websites and advertisers access that data. The legislation would complement a pair of privacy bills in the House that are aimed at protecting financial and health data.



Hillary Clinton Steps into BlackBerry Negotiations

The Obama administration will mediate negotiations between BlackBerry-maker Research In Motion (RIM) and foreign governments that want to ban the smartphones for security reasons. The United Arab Emirates, Saudi Arabia and other countries want to block certain BlackBerry services because Canada-based RIM won't give them access to encrypted customer data. The governments said they need access to potentially threatening IMs and emails. U.S. Secretary of State Hillary Clinton told *The Wall Street Journal* that there's a "legitimate security concern, but there's also a legitimate right of free use and access."

Misses



Anti-tracking Feature Unused by Microsoft

Microsoft, maker of the world's most popular web browser, included a privacy-friendly anti-tracking feature in its Internet Explorer 8.0. But the company opted not to make its use automatic—allowing advertisers to follow users' surfing habits. The feature exists, but it must be turned on each time the browser is opened. *The Wall Street Journal* reported that product designers lost a key 2008 internal battle with business executives who said the well-regarded privacy feature would crimp online advertising profits. The decision leaves Explorer users more vulnerable to potential misuse of information.



Health Care Data Vulnerable

The health care sector remains highly vulnerable to data security breaches because of weak internal controls. Case in point: A Houston doctor's laptop, with personal information of 1,600 patients, was stolen in May. The computer theft was the third such health-care-related security breach in the Houston area this year, the *Houston Chronicle* reported. Officials at Texas Children's Hospital and Baylor College of Medicine have begun to alert patients whose information may have been compromised. Files with their names, birth dates, diagnoses and dates of service were on the hard drive.



Rite Aid Reaches \$1 Million Settlement with FTC

Rite Aid Corp. settled allegations that it violated government privacy rules in a \$1 million agreement with the Federal Trade Commission. The drugstore chain was accused of failing to protect customers' health data after news reports showed it was dumping records in unsecured areas, according to *The Wall Street Journal*. The company will set up an information security plan and pay for a third-party audit of its procedures every two years to ensure it meets its own guidelines. It faces further U.S. Department of Health and Human Services scrutiny on record disposal under the Health Insurance Portability and Accountability Act.



Q&A: Family Fraud

Vicki Volkert, Identity Theft 911 Fraud Specialist

We asked Vicki Volkert—who has investigated financial and retail fraud for nearly 30 years—what to do if a friend or relative steals your identity. Her short answer: Do the hard thing. Set aside bad feelings. Focus on getting back your good name and credit.

Q: My cousin stole my identity to open credit cards, buy a new cell phone and rent an apartment in my name. I was rejected for a car loan, and now I'm worried about my credit score. Is this a crime?

This is definitely a crime, and it happens more often than you'd think. Most identity theft is committed by someone who knows the victim and has easy access to personal information—we call it familiar fraud. Parents sometimes commit identity theft against a child, usually in a divorce, when finances are tight. I've seen it happen between fathers and sons, mothers and daughters (especially when they have the same or similar name), brothers, boyfriends and girlfriends, roommates, co-workers.

I can't believe she did this to me. What should I do?

Most people in your situation feel a deep sense of betrayal. They're angry—but they're also torn, because it was someone they love and still care about. Victims are often reluctant to prosecute and may get pressure not to from family members. You can't control family dynamics, but you can focus on the necessary steps to clean up your credit report. If you don't, you could have financial trouble for years to come—like being denied for that car loan, or even a mortgage.

Should I file a police report? I don't want to get her in trouble or upset my family.

Only you can decide whether or not to file a police report (and there's no predicting how the police would handle the case), but the companies that extended credit in your name think you owe them money, and they will pursue it. If you're asking them to take the loss and release you from responsibility for the debt, you must prove to them that you're a victim—and that you're willing to help. Creditors will want a police report; proof of your identity and address; and documentation showing where you lived at the time of the fraudulent activity. They may also want you to submit a written statement asserting that you are a victim of identity theft and to identify the perpetrator of the crime. If you're not willing to pursue the perpetrator through law enforcement, you can still attempt to resolve the situation, but you're more likely to have to pay the debt yourself.

Contact the creditors and tell them that you did not open those accounts. They will tell you what steps to take next. Do not pay the debt or make payment arrangements with your cousin; doing so will ratify the accounts and make you responsible. Check your credit report with all three reporting agencies and have each put a note (consumer statement) in your file about the fraud. You may want to request a seven-year security alert (requires a valid identity theft report from law enforcement) or a credit freeze to prevent your cousin from continuing to use your credit. If you're going to file a police report, do it right away. You can also complete an identity theft affidavit with the FTC to provide to creditors. (Victims who were underage when the credit was established can use their birth certificates as documentation.)

Identity theft is bad enough when it's committed by a stranger. When it's someone you know and trust, it's devastating. Right now, set those feelings aside and concentrate on the steps you're willing to take to clear your name.