The New York Times

December 21, 2003

Dumpster-Diving for Your Identity

By STEPHEN MIHM

Stephen Massey was only a few minutes late, yet he apologized profusely as he strode into the lobby of a crowded restaurant in downtown Eugene, Ore. "I'm very punctual about my time," he said, clasping my hand in a firm shake. With his freshly combed hair, crisp white shirt and trimmed mustache, he looked like an off-duty cop or fireman -- a "pillar of the community," as he later described himself, a wolfish smile playing across his lips. Far from it: Massey, 39, directed one of the most extensive and notorious identity-theft rings prosecuted so far by federal authorities. By the time investigators broke the case, Massey and his partner in crime, a computer whiz named Kari Melton, had ruined hundreds of people's credit. A judge sentenced them to prison in 2000; Melton was released in 2001, Massey the next year.

The Federal Trade Commission estimates that identity theft costs nearly $53 billion annually. Some seven million people were victimized in 2002. Yet little is known about how the perpetrators actually operate. It's a popular perception that most identity theft happens on the Internet, but over the course of dinner, Massey quickly made clear that low-tech methods of getting people's personal information are far more effective. "Every day was exciting," he recalled between mouthfuls of potato skins. "We went to Vegas, Atlantic City. We made a business of it. It was like James Bond . . . 'Mission: Impossible.'"

In late October, Massey disappeared, violating the terms of his supervised release and prompting a national warrant for his arrest. It had become clear to me in five months of interviews that not everything he said was to be trusted, although much of it was verified by the detectives and prosecutors who had already investigated his crimes and by Kari Melton. As for Massey's current whereabouts, Steve Williams, a detective in the Eugene Police Department, who worked on the first case against Massey and is once again on his trail, said: "My gut feeling is that he is in the Seattle area" -- where he has family -- "back to his old tricks, doing drugs, identity theft and counterfeit checks."

If Massey has indeed resumed operations, it's a sure thing that he's not working alone. His identity-theft crimes depended on the work of a carefully built ring, one that employed hordes of petty thieves and drug addicts. If he sticks to his old techniques, his crimes will originate in Dumpsters and garbage cans, where information can be culled from discarded personnel files and other trash. It's not the most glamorous crime, but that doesn't make it any less devastating to its victims.

Discovering the Dump

Massey's life began to unravel in his late 20's, soon after he started experimenting with the highly addictive stimulant methamphetamine. Before that, Massey achieved some semblance of success, managing an awning-maintenance company, marrying and, with his wife, having two daughters. Then he and his wife divorced in 1992. Soon after, he remarried, and divorced a year later. His business began to decline. Sometime in the mid-90's, his teenage girlfriend offered him some meth. "So here I am with

Exhibit G

no place to live, on the rebound and with a habit," Massey recounted. "Who wants to look for a job again?" Massey began hanging out with a much younger crowd of meth addicts, called "tweakers," and forging checks to feed his drug use. It was during this time that he began to wonder if he could hijack people's identities for profit. He stumbled onto the answer soon after, when the meth-heads invited him to go "Dumpster diving" for junk. Massey and the teenagers piled into his Ford Explorer and drove to the outskirts of Eugene.

"It was the first time I had ever been to the dump," Massey recalled, wrinkling his nose. "I said, 'I'm not going to get dirty,' so I wandered over to a shed where the recycling was stored. I notice there's a big barrel for recycled paper that's full of discarded tax forms from an accounting firm." Each form had the person's name, date of birth, Social Security number -- all the information necessary for taking out a line of credit.

"The wheels started turning in my head," Massey said, smiling. "The guys profiled here were pulling in $800,000 a year. So I told the tweakers to get all this stuff in the truck. Now! I said, 'This is worth five million right here.'"

Growing the Business

For the aspiring identity thief, a Dumpster can be a gold mine -- full of documents discarded by hospitals, accounting firms and law firms. And if that doesn't work, there are other readily tappable sources. "Theft from mail is also a very common mechanism for getting this stuff," explained Jonathan J. Rusch, the special counsel for fraud prevention in the Department of Justice. "Even one handful of mail can yield lots of valuable information to an identity thief." Rusch recalled a recent case in Southern California in which an identity thief robbed postal drop boxes while driving a bogus mail truck. Total losses: $1.7 million.

Some identity thieves do go straight to the Internet, hacking into databases or using "phisher sites" -- phony Web pages that mimic real banking and e-commerce sites in order to entice victims to hand over sensitive information. But those cases remain the exception, not the rule. For the most part, obtaining dates of birth and Social Security numbers still begins off line, and often in the trash.

The digital dimension usually comes into play later. After harvesting information from a Dumpster, Massey would visit a credit clearinghouse online and apply for credit in the person's name. Massey would enter the person's existing address, and when asked whether the victim had moved in the past two years, Massey would type in a new address, a temporary mailbox rented for the occasion.

"It would ask me if I wanted an additional cardholder on the account," he said, walking me through his scam. "Absolutely -- I would!" he said, mimicking typing on a keyboard. He would put his name down. Both cards would come in the mail, one in the victim's name and one in his. This second card, made out to S. Massey, enabled him to use his own identification when making purchases -- while the first initial also offered some measure of anonymity. He could now use the victim's credit as he saw fit.

Massey met Melton, 34, shortly after his first visit to the dump. She owned a company that issued travel permits for oversize trucks; like Massey, she had started taking meth and drifted into petty crime. Melton was already creating bogus checks on her computer -- all she needed was a quick over-the-shoulder glance at someone's account number as he paid for groceries and she could generate some fast cash. But she, too, had been looking for a way to parlay identity appropriation into bigger profits.

One day she visited a friend's house; Massey happened to be there, typing away. "He has this laptop on

the table," Melton recounted over the phone. "Most of the people in the underground were computer illiterate, but he knew about computers, so we had something to talk about." They quickly became friends and found they had something in common besides computers and meth use. "We both enjoyed having money and both enjoyed not having to hustle for it," Massey said.

The schemes developed by Massey and Melton did not initially have a name. Existing federal legislation addressed only the fraudulent creation, use and transfer of identification documents, not the theft and criminal use of the underlying personal information, particularly Social Security numbers and dates of birth. That changed on Oct. 30, 1998, with the enactment of the federal Identity Theft and Assumption Deterrence Act. The new law gave prosecutors better tools to prosecute everything from check forgery to the misuse of someone's credit card to the kind of scams perpetrated by Massey and Melton. The law, like similar legislation passed by several states around the same time, gave a common label -- "identity theft" -- to a constellation of crimes previously prosecuted under different names.

But the class of crimes committed by Massey and Melton are far more devastating than garden-variety identity theft. If someone steals a credit-card number and racks up charges, the card is canceled, and the victim walks away chastened but unscathed. But if the identity thief borrows the victim's Social Security number and obtains credit in the victim's name without his knowledge, that's another matter altogether. In many cases, these victims don't realize someone has preyed on their credit until the thief has bled them dry. According to a Federal Trade Commission report released in September, it takes 26 percent of victims between one and five months to realize the imposture; another 12 percent do not learn for at least six months, if not longer. By that time, the damage to a person's credit can be complete.

Worse, even if the victim or the credit-card companies figure out that an identity thief has taken out an illegal card or loan, and cancel the fraudulent account, the identity thief is rarely apprehended. "The banks never come after you -- they just stop the card," Melton explained. "No federal investigators. You just throw away the card and know not to do that bank again."

Part of the problem is jurisdiction. Jonathan Rusch of the Department of Justice sketched out a typical course of events: "I live in Washington, D.C. Let's say I find out that someone has opened credit accounts in my name with companies in South Dakota. I can go to the Washington Police, but the credit-card company is in another state. Many departments are reluctant to take police reports because they don't think they can investigate these cases themselves."

The feds, on the other hand, have the resources, but few cases are large enough to warrant an investigation. Those that do face serious obstacles. Sean Hoar, the assistant United States attorney who prosecuted Massey and Melton, gave me an example: "We follow the money by following the Internet-protocol addresses." But he explained that identity thieves are well aware of this problem and cover their tracks, juggling modems, computers and software. And Internet service providers have no obligation to retain the kinds of records that might form a paper trail of a thief's activities.

How bad, then, is the problem? Avivah Litan is pessimistic. An analyst with Gartner Inc., a research company that advises financial institutions on security issues, Litan speculated that fewer than 1 in 700 acts of identity theft end with the conviction of the offender. It may be worse: "People in the industry whom I've talked to have said it's more on the level of one out of a thousand." Identity theft, she lamented, "is a very lucrative, low-risk crime."

Refining the Scheme

One in 700. One in 1,000. Figures like these go a long way toward explaining how a pair of identity

thieves like Massey and Melton operated with impunity for so long. Their yearlong buying binge came to an end only after an accomplice was picked up. In other words, the police got lucky.

Until their capture, the duo practiced increasingly refined versions of Massey's original scheme. They ordered secondary credit cards made out to S. Massey or K. Melton. In time, they purchased equipment for making fake driver's licenses, allowing them to fully assume another person's identity. They shared resources, though each cultivated a separate set of victims. Melton explained: "We did the same crime at the same time in the same room -- but we didn't do it together. We had different accounts. He had his, and I had mine." Working side by side, they repeatedly scavenged information on an individual and then went online and did a credit check. "It costs, like, $12 to $30," Melton explained. This was a negligible expense; it was paid for, after all, using other people's credit cards. And it ensured that the victim was someone with assets.

"I would know what I'm dealing with before I'd invest time in the person's Social Security number," she went on to say. Part of that decision depended on whether the prospective victim owned a home. A typical homeowner can get an instant credit line of $5,000 to $25,000. Melton told me: "If you have the credit to get a home loan, you have the credit I need."

If the victim passed this test, Melton or Massey would begin applying for credit cards using one of the many online credit-card sites that give automated responses to requests for credit. One site, which is now defunct, "let people apply online and get an instant answer within 30 seconds," Melton explained. "I would have $1,000 available to me instantly" -- along with the promise of a credit card.

Massey or Melton would then have the card sent to a temporary mail drop. To answer queries from the credit-card company, they provided the number of a prepaid cellphone. "There was a time when I had 15 cellphones plugged in all the time," Massey claimed. "I had notes saying what phone was for what." Each time a phone rang, Massey or Melton would check the note, pull the matching credit report and answer in the appropriate tone of voice. Investigators estimate that they opened more than 400 fraudulent lines of credit during their spree.

Once they had their system set up, Melton rarely paid for things in person. Part of the reason had to do with race. In Eugene, a black woman stands out. "I couldn't hide if I wanted to hide."

Massey, on the other hand, enjoyed playing the part of an impostor and talking his way out of tight situations. "That's one thing they teach you in the Fire Department: 'Never panic.'" Melton put it this way: "Steve is a con man, a great con man. He's the kind of guy who can sell you anything." But, she cautioned, "he's kind of a liar."

Indeed, any conversation with Massey yields a blend of fact and fiction. At different times, he told me that he had worked as a firefighter, earned a bachelor's degree in business management and been elected a city councilman. In reality, he signed up to volunteer as a firefighter but was dismissed within months, attended community college and never earned a degree and as for being a city councilman -- well, never mind. In court records, a psychologist described Massey as suffering from "narcissistic tendencies." It's almost as if Massey's desire to be important could be satisfied only by stealing other people's identities. He wanted to be someone, desperately. And indeed he did -- by becoming someone else. "I was an actor," Massey told me. "I could put on a new hat every day. Who do I want to be today? The feeling after you've just hooked them, is just, like, bam!" He smacked his fist into the palm of his hand. "Take that, Bank of America!"

All the Young Tweakers

Like many identity-theft rings in the United States, Massey and Melton's enterprise employed scores of petty criminals addicted to methamphetamine. "It's a very typical combination," Hoar, the federal prosecutor, explained. "The meth user tends to be more prone to this type of behavior than other drug users." To a person on meth, tasks that might otherwise seem boring -- like sorting thousands of tax forms or reconstructing shredded patient records -- are said to become oddly enthralling. Meth could turn slackers into hyperefficient paper pushers. "Drug addicts who used to kick in doors and steal electronic devices now kick in doors and steal identity information," Hoar said. "They do it because identity information is more transferable and lucrative than stolen electronics."

Word spread among the tweakers that Massey and Melton would swap meth, cellphones and other goodies for people's Social Security numbers and dates of birth. "We made a business of it," Massey said. "The tweakers came to work at 8 o'clock every morning. I gave them bonuses. I treated them like employees."

The "employees" collecting identification information fell into several categories: "bucklers," who broke into cars; "criddlers," who stole, from, say, mailboxes; and Dumpster divers, who rooted through garbage from hospitals, accounting firms, banks, law firms and other organizations known to be careless with personal information. Massey also employed a select few to transcribe documents onto neatly labeled 3-by-5 index cards.

Both Massey and Melton brought business expertise to their enterprise: Massey had managed a handful of employees at the awning-maintenance company. Melton had started her travel-permits company. They were adept at managing a ring of subordinates. "I felt like this big, old king banana," Massey boasted at one point. "I was like the Pied Piper and the music man to these kids on meth." Melton was much more cautious, but, as she recounted, "Steve would bring any ragamuffin into the hotel room to watch what we were doing."

Getting Deep Inside

Steps have been taken to protect consumers from identity theft, but too often they fall short. The Financial Services Modernization Act of 1999 required that financial-service and insurance companies safeguard information, but the law does not apply to hospitals or universities, for example. Yet even if every business in the country never threw away a single scrap of paper, thieves would still be able to steal Social Security numbers using inside contacts. Some gangs of identity thieves have relied on cleaning crews and temps with easy access to sensitive information.

More dangerous still is what Joanna Crane calls the insider threat -- when an actual employee does the dirty work. Crane, who manages the Federal Trade Commission's identity-theft program, recently noticed this trend while updating a database of cases: "A growing number of consumers complained that information had been compromised due to theft of company records." Last year, a case made the front pages: the theft of more than 30,000 credit histories from Teledata Communications Inc., an intermediary between businesses and credit-reporting agencies.

According to prosecutors, a short-term employee named Philip Cummings funneled credit histories to Linus Baptiste, a front man for a gang of identity thieves, many of them operating in New York City. Baptiste sold each report for up to $60 and split the proceeds with Cummings. When Cummings left the company in 2000, he took with him copies of the proprietary software and the necessary passwords, and he and Baptiste downloaded reports from afar. The extent of the fraud remains unknown, if only because many of the identity thieves who used the data remain at large.

Insider identity theft is especially common in Delaware, home to a number of financial-service companies. Beth Moskow-Schnoll, an assistant United States attorney based there, says that thieves who approach employees have very specific requests. "Here's what I want," she said to me, pretending that she was talking to someone on the inside. "I only want cards with a credit limit of $5,000 or more." Other thieves approach employees of banks and credit-card companies requesting that they pull information on people living in wealthy neighborhoods.

Insider cases have surfaced throughout the country: a human-resources employee in Illinois who harvested the identities of up to 80 co-workers, an office manager at an H&R Block office who stole information from his customers and a medical assistant who pilfered information from patient files at a hospital.

While the actual thieves are to blame, the companies safeguarding these records should share responsibility, experts say. "There is no 'standard of care' to which these companies are held," said Litan, the Gartner Inc. security analyst. "If someone in the organization steals credit reports, the company is not responsible. The bottom line is that the banks and financial institutions are not held liable." Melton, for her part, doesn't think there's much to be done. "All you need is some idiot, some young kid working at a hospital or bank who's not happy with his job, who's not making enough money. He'll sell you Social Security numbers."

The Trail of Fraud

By the time Kari Melton and Stephen Massey entered federal prison in 2000, they had created a convoluted trail of fraud that proved almost impossible to reconstruct. "It was insane," Detective Williams said as he unpacked boxes of evidence from the case in a windowless room in the Eugene Police Department. Williams guessed that the true extent of their crimes may never be known. Part of the reason had to do with the thieves' peripatetic lifestyle. Wide awake, wired and constantly collecting new identities, they wandered from Eugene to Portland to Las Vegas and back again in a roaming tour of fraud and imposture, paying for everything -- plane tickets, car rentals, hotel rooms, restaurant meals -- with the credit of others.

Over the course of the year, they racked up a remarkable record of debt thanks to other people's credit. By Melton's reckoning, the amount is higher than what prosecutors estimated. "The claim that we stole hundreds of thousands isn't true," she told me. "It was more like something over a million."

Massey and Melton burned through credit as fast as they acquired it, satisfying every whim and desire. Williams showed me receipts from some of their purchases. "Highly overpriced food," he muttered, handing me a receipt. It was from Omaha Steaks and listed an order for a filet mignon, a stuffed sole with scallops and crabmeat, jumbo shrimp, a smoked-salmon roll, a Black Forest cheesecake and a dessert described as a "chocolate ecstasy cake." Total bill: $387.45.

But that purchase pales next to purchases of jewelry, perfume and other luxury goods. Buying them often became an end in itself. As Melton recounted, they would challenge each other: "O.K., Steve, it's 2 o'clock. Let's see who can have a Rolex watch delivered here by tomorrow morning." And on it went: trips to Vegas to gamble, gorge and hole up in a hotel room, pushing the credit envelope.

Massey and Melton enjoyed spending time in Vegas, and not just because they could gamble on someone else's dime. Usually, $1,000 cash advances raise red flags, but in Vegas that amount didn't invite suspicion. While the casinos helped Massey and Melton extract cash from credit, the duo also began experimenting with ways to wring more out of every line of credit. The key to keeping credit

cards in play for longer periods of time, according to Massey, was to shift credit from one account to another in a complicated pyramid scheme. "You can pay your credit card with another credit card," Massey said and laughed. "I've always loved that. When we would get another batch of credit cards that came with checks, we would pay the ones that were overdue." Or, Melton added: "If I got a credit card with good credit, and it lasts more than a month, I'll pay the bill. Then, after a few months, I can upgrade the credit. A couple months later, I'll use it."

Over time, their working methods began to diverge. While Massey continued to cull identities from the conventional sources -- garbage, recycling, stolen mail -- Melton experimented with more esoteric means of harvesting information: for example, she used a "sniffer program," one that allows a hacker to eavesdrop on someone else's keystrokes. She also began to impose ever greater security on her operations, downloading encryption programs from M.I.T. to protect her accounts.

Melton grew more careful as Massey got sloppy. "After I surpassed Steve, he started learning from me," Melton claimed. "I didn't like his organizational style, the women he had in the room. He was into prostitutes, but not even good-looking ones! They were just sitting there watching us do felonies."

Massey's downfall came, much as Melton feared, at the hands of one of his subordinates. Massey and a few hangers-on were staying at the Hilton in Eugene. Four tweakers burglarized a car in the hotel parking lot. When a security guard approached, one of them ran up to Massey's room -- inadvertently leading the police to their ringleader. And once he and the tweakers landed in jail, it was only a matter of time before they found Melton. After a week of interrogation, Williams had enough information to track Massey's partner down to a nearby motel.

Back in Business?

Massey went to prison for 41 months, Melton for 15. Once they got out, each was assigned to the same probation officer. But there the similarities end. Melton has had some success in starting a new life, but Massey's problems began soon after he was released. The police picked him up earlier this year with equipment for forging checks in his Ford Explorer. The charges were eventually dropped; Massey went into a halfway house, only to be kicked out for violating regulations. Unfortunately, Massey's request to be on supervised release near his parents in Washington State went unheeded, and he ended up back in Eugene, near his old haunts.

"The circle of friends is still there," he said before he disappeared. "I'm approached -- I kid you not -- maybe three or four times a week by people wanting to do identity theft." He said then that he turned them down. "There's a lot of pressure," he lamented. "There's not a day that I don't think, Man, three days and I could make a living." By October, the pressure proved too much for Massey. He was implicated in a forged-check scheme, and detectives suspected that he was taking meth again. The U.S. District Court in Oregon ordered Massey to wear a monitoring bracelet. But shortly before being fitted for it, he disappeared. Massey's federal probation officer, Mark Walker, realized he was on the run when he made an unannounced house visit on Oct. 30 and a neighbor reported that Massey had left days earlier.

Melton, for her part, will soon earn a degree at her local community college as a computer-networking specialist and says she hopes to get a bachelor's degree eventually. She has thought about starting her own business, parlaying her computer skills and her former life into a more legitimate profession. If she goes that route, she might consider work as a security consultant. The incidence of identity theft is skyrocketing: the number of complaints received by the F.T.C. has nearly doubled every year over the past three years.

Worse, the identity thieves are becoming more and more technologically savvy. Sean Hoar sees a new era of identity theft dawning, one that is far more sophisticated and difficult to prosecute. "You will still have street-level criminals in the Internet age," he said, including Massey in this group. "But you will also have more disciplined and sophisticated individuals who utilize the Internet." In one well-publicized case, an identity thief based in Chicago set up a fake Web site and sent e-mail messages to users of Microsoft's MSN Internet service, asking them to visit the page and update their account information -- including, of course, their credit-card numbers.

At the end of the last dinner I shared with Massey, the conversation turned to these more sophisticated scams. His eyes lighted up. "The scams are getting more unique," he said as he polished off a slice of cheesecake. "I hate to say it's cool, but you have to sit back and admire these scams. It's just amazing." He paused for a moment, lost in reverie. "Right when you think all the scams have been used up . . . there's another one."

Stephen Mihm is the Newcomen postdoctoral fellow at Harvard Business School.