Who's really in your office?

Medical ID theft on the rise – don't be a victim

BY STEPHANIE STEPHENS

The so-called "Beauty Bandit," Maria Chrysson, 29, was charged early last month with grand theft and scheming to defraud. Around the same time, "Botox® Bandit" Jamie Merk, 32, and Kellie Thomas, 23, were each charged with grand theft in separate incidents. Shatarka Nuby, 29, faces credit card fraud charges. What links these women is the fact that the charges lodged against them all revolve around cosmetic procedures – and the alleged identity theft used to obtain the procedures for which they had no intent of paying, according to law enforcement officials.

The above examples represent only a small sampling of recent incidents relating to identity theft and plastic surgery – but they seem to be accelerating with frightening speed.

Life was so much simpler for plastic surgeons in the days before rampant identity theft.

"Many years ago, a patient passed me a fraudulent check. That person went to jail," recalls ASPS member Scot Glasberg, MD, New York. Just a decade ago, it seems that detecting and preventing fraud was much easier, as perpetrators usually needed assistance from the criminal underworld to procure a false identity and more often than not left a paper trail.

Fast-forward to early 2009 and a phone call fielded by Larry Nichter, MD, Huntington Beach, Calif. "How ***dare*** you use my credit card?" the caller yelled. "Look at the amount! That's fraud! You can't do that!"

But Yvonne Jean Pampellone could use the credit card – and she did. It was a classic case of identity theft used to obtain cosmetic surgical procedures.

Unwanted publicity

Pampellone, a 30-year-old woman from Laguna Niguel, Calif., who would soon be dubbed the "Boob Bandit" by southern California news outlets, had opened a line of credit in someone else's name and, in September 2008, she underwent $12,000 in breast augmentation and liposuction procedures performed by Dr. Nichter.

Dr. Nichter became concerned when the fictitious "Cindy" skipped her follow-up appointment. "Did she die, have an emergency or see another doctor? The idea of risking one's own health and life to get away with surgery was one thing, but who was doing follow-up care and removing stitches? To me, disappearing like that was just unbelievable," he says.

"Pampellone wasn't your typical robber type," Dr. Nichter adds. "She was bright and very articulate," not someone you'd immediately flag as a thief, and the Social Security number she presented matched the one on the fraudulent credit card she'd given to his staff. However, her male accomplice – who was introduced as her boyfriend – seemed oddly disconnected and self-absorbed, he adds.

The plastic surgeon contacted the Huntington Beach Police Department and began researching the incident on his own. But working against his sleuthing efforts was the fact that the office was quite busy that day, and his closed circuit surveillance system – which normally erased tapes after two weeks, long after Pampellone's plot was apparent – hadn't been working.

Still, Dr. Nichter cleverly used identification numbers on the implants that he removed from Pampellone prior to her new augmentation. From those, the original surgeon was located, and Dr. Nichter's surgery center staff took the name he supplied and identified Pampellone from a photo lineup. The Huntington Beach police had enough information to be granted an arrest warrant.

Pampellone ultimately turned herself in and pleading guilty to burglary, grand theft and identity theft. She received a sentence of 180 days in jail and three years' probation.

Once bitten, Dr. Nichter is now more than twice shy, having implemented stringent identification procedures in his office. "It can still happen," he says.

You must do more

The nonprofit, research-focused World Privacy Forum notes that medical identity theft is the fastest-growing form of identity theft. The perpetrator uses another person's name and occasionally other parts of their identity – such as insurance information – without his or her knowledge or consent, to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods.

Medical identity theft also can create profound administrative headaches in addition to financial burdens: It frequently results in erroneous entries into existing medical records and the creation of fictitious medical records in the victim's name.

A national survey released in April by privacy think-tank Ponemon Institute calculates that 1.42 million Americans have been affected by medical identity theft, with $28 billion in related costs. Javelin Strategy and Research's 2010 study counts more than 11 million new victims in 2009 alone.

What to do? According to Laguna Niguel, Calif.-based attorney and Certified Information Privacy Professional Mari Frank, The Fair and Accurate Transactions Act of 2003 directed the Federal Trade Commission (FTC) to create the "Red Flag Rule" finalized in early 2008. (Enforcement of the Rule has been delayed until Dec. 31.)

Frank, who is also the author of *The Complete Idiot's Guide to Identity Theft*, explains that "these rules would require the financial industry and others to establish policies to help to prevent and mitigate identity theft. Even doctors who extend credit are subject to them. The FTC also tried to apply the Red Flags Rule to attorneys, alleging that those who take retainer fees are extending credit. The American Bar Association fought this in a lawsuit and won, but the ruling is on appeal by the FTC."

The AMA filed a similar lawsuit in May, hoping the courts will find physicians exempt.

Should the court rule against the AMA and physicians be required to observe the Red Flags Rule, "any failure to comply could be considered as negligence in any legal action," Frank warns. "Additionally, many insurance carriers require that doctors and others adhere to the Red Flags Rule and best practices to prevent identity theft."

Assume nothing

The World Privacy Forum warns that "services provided to thieves will not be covered by insurance, and providers can lose revenues or have un-reimbursed expenses." Provider costs can be significant, as can legal liabilities associated with incorrect records, and complying with the Health Information Privacy and Portability Act isn't enough, some experts say. Physicians need to be ready to recognize relevant red flags; prevent and identify ID theft; and consistently update their privacy and health information computer programs and office policy.

Medical identify thieves can be articulate and charming. They're often females in their 30s, perhaps a single mom without enough money to fulfill appearance aspirations, Frank says. Identify theft is viewed as a low-risk, high-reward endeavor: Only about 10 percent of identity theft cases are investigated – and of those about 10 percent are prosecuted. Frank calculates that 12 percent of ID theft is committed by someone the victim knows, and half of those involve family members.

"Doctors must be vigilant about verifying new patients and making sure that when credit is extended, the address on the credit report matches the one given by the new patient," Frank says.

A fraudulent applicant won't present the victim's address, since they don't want the victim to know they're being swindled. Most creditors, though, really don't worry about an alternate address. "People move all the time," Frank says.

She applauds Dr. Nichter's diligent initiatives to seek justice.

"If physicians deliver evidence to police on a silver platter, the case may be prosecuted," says Frank, who's a reserve in the Orange County, Calif., Sheriff's Department. "With so many other heinous crimes taking place, many departments don't have the resources for such a labor-intensive investigation."

No excuses

A plastic surgery practice that partners with a health-care financing company such as CareCredit (a company endorsed by ASPS) and extends financing essentially is verifying that the person applying is, in fact, *that person*. Therefore, it's essential to take steps to get it right.

"Always make sure staff checks at least two forms of ID, including driver's license with picture, against the credit card being used to pay for the procedure," says Tony Seymour, CareCredit senior vice president of practice development. CareCredit, he says, carefully monitors and researches disputes by cardholders claiming that one of its cards had been charged for procedures the holder may not have undergone.

When accepting credit cards, you may not copy the driver's license, but you *can* view it, adds Frank. When someone applies for credit through your office, you may copy the license.

"Sometimes, when we call the doctor's office, not only didn't the office check identification, but it didn't obtain the required signature on the sales slip," says Seymour. "A majority of fraud is preventable, but offices need processes in place to prevent it."

Specific language is also included in the agreement, and policies and procedures are in place from CareCredit that delineate what's required at both point of sale and

Continued on page 60

Raising red flags

The Red Flags Rule is an identity theft-prevention mandate that requires "creditors" – including plastic surgeons and other physicians who regularly bill their patients for services rendered – to implement extra steps to protect customers' (or patients') identities. Creditor status is assigned if physicians regularly extend, renew or continue credit and offer covered accounts to patients. (A covered account involves multiple payment or transaction options.)

According to the Federal Trade Commission, the Rule provide all financial institutions and creditors the opportunity to design and implement a program appropriate to their size and complexity, as well as the nature of their operations. A roster of 26 possible red flags falls into five categories:

- Alerts, notifications, or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personally identifying information, such as a suspicious address
- Unusual use of – or suspicious activity relating to – a covered account
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

The FTC has delayed enforcement of the Rule until Dec. 31. For more information, go to *RedFlags@ftc.gov*. PSN

RISK TIP

The ugly side of social networking

Social networking tools like Facebook can make communication with family and friends easy and instantaneous. Perceptions of privacy, however, may be false. In May, Facebook users were informed that chats and e-mails previously thought to be private in several hundred thousand profiles were, in fact, visible to others. Such breaches could be destructive for a plastic surgery practice, and while it might be tantalizing to use this tool to connect with patients, the qualities that make Facebook simple to use can create problems for medical practices.

Before creating a Facebook page or connecting your personal profile to your practice, consider the following:

- Assume all your comments on the Internet are public, permanent, and discoverable in litigation. If one word of your posted communications is related to a case, all of it is discoverable.
- Avoid "friending" patients, unless they were your offline non-patient friends before Facebook. Avoid postings and links that may not reflect favorably on your profession.
- Avoid giving advice or discussing medical or financial information on Facebook.
- Remember that discussions inside Facebook among friends are visible to others.
- Prevent the unintended use of your comments, links, and thoughts. Facebook uses programs that actively link any postings, profile information, and links to external sites. Privacy settings are tricky with social media sites, and change rapidly.

In response to the growing risks and mounting penalties related to breaches of patient data and financial records, The Doctors Company has created CyberGuard℠– a free service for its member physicians. The coverage protects physicians from a privacy breach through a social media sites like Facebook. For more information, visit thedoctors.com/cyberguard. PSN

Contributed by The Doctors Company. For more risk management tips, articles, and information, please visit *thedoctors.com/knowledgecenter*. Visit *PSNextra.org* for a new practice management tip every day.

ID theft

Continued from page 26

point of application, adds Mindy Karro, the company's senior vice president, marketing. "It's of paramount importance to us to ensure the practice knows how to protect itself," Karro says. "In the event of a customer complaint, as long as the office has followed all policies and procedures we've trained them on, CareCredit accepts responsibility."

The potential for human error can't be discounted, however. "We try to train every office with which we do business to follow these procedures, and we provide desktop tools, in person follow-up and reminders on requirements to help practices – especially those with high turnover – do everything possible to prevent fraud," Seymour adds.

"Physicians need to go further: Get the patient's cell phone and e-mail address," says Karen Zupko, a practice management consultant who runs the Chicago-based KarenZupko & Associates Inc. She's adamant that plastic surgeons realize this isn't just about plastic surgery – ID theft has huge ramifications for the uninsured. "People are giving their insurance cards to others with dire consequences," she says.

Zupko also worries about practices desperate to book cases in this challenging economy. "They forget you can do the case and not get paid," she says. "When a patient objects strenuously, remember Shakespeare's *Hamlet*: 'Methinks the lady doth protest too much.' Go ahead and push hard for information. There's a tradition in plastic surgery of talking about money. If you lose a fraudulent patient, you've actually won."

And if you're tired of no-shows, Zupko wants you to get tough. "You ask for a surgery deposit. Ask for a credit card when scheduling, especially for consults."

'In Texas, they call 'em *runners*'

Jessica Burd, practice manager of Advanced Cosmetic Surgery Center in Aurora, Colo., knows her practice isn't required by law – yet – to "really verify" identification. "It's easy to assume 'they' are who they say they are. At 100 percent self-pay – patients don't submit insurance claims – it's a really big gray area for us."

Burd's staff records patient date of birth, social security number and, like Dr. Nichter, takes patient photos. Still, the practice has been burned – and not because the staff is unaware. One impostor patient toted a completed credit application, persistently demanded surgery the next day, and was accommodated.

"That was a real red flag: finance and a quick-moving case," Burd reflects, admitting that, conversely, sometimes patient circumstances can appear fuzzy while being absolutely on-the-level. "These fraudulent patients are very manipulative. If you say 'no,' they'll make it look like you're being unfair.

"We're in a luxury sales business, where it's really hard to make patients jump through a lot of hoops. They think: 'If you don't trust me, why should I trust you?' "

Still, trust only goes so far, especially when a "dine-and-dash" mentality is prevalent. "We have had this happen, mainly with fillers," reports ASPS Member Surgeon Mary Gingrass, MD, Nashville.

The first line of defense for many of your colleagues is to have patients pay in advance unless they're known, repeat customers. Such tactics are favored by Rod Rohrich, MD, professor and chairman, Department of Plastic Surgery University of Texas, Southwestern Medical Center. "In this way we prevent the 'runners,' as we call them in Texas."

Stories are also traded about doctors who put buzzers on their doors to slow patient exits.

The first clue in August 2007 for Burt Rademaker, MD, was that his client flatly refused his aesthetician's request for a photo before a facial procedure. When Jaimie Merk returned to Dr. Rademaker for Botox®, he thought, "I'm taking a picture, like it or not."

Appearing at his Rejuva Center for Plastic Surgery and Med Spa in Westchase, near Tampa, Fla., Dr. Rademaker describes Merk, now age 33, as "very sophisticated and delightful. I didn't think she was up to any mischief." The exuberant patient told the desk to hang on while she ran to get her credit card. Instead, she ran from approximately $850 in procedures. Merk was gone for 20 minutes; 30 minutes; and then, forever. Thus was born "the Botox Bandit," a term that resonated around the globe.

A July 2009 story in the *St. Petersburg Times* notes Merk is now "on probation until 2012 for several convictions of grand theft and worthless checks in Hillsborough and Pinellas counties." She had also bilked at least one other clinic in Florida and moved on to New York City for further fraudulent touch-ups.

"At first, I was pretty upset. Then I was on CNN within 48 hours," Dr. Rademaker says. Like colleague Dr. Nichter, his anger was tempered by his ethics. "We're in business to be compassionate, empathetic. We want to help. The trust element is there and we're not looking right away for someone to steal from us. It's a whole new way of stealing. I don't want to get stung again."

Sad but true, he figures, that some people repeatedly need change in order to feel better. "I can understand stealing clothes and food, but Botox?" PSN

Editor

Continued from page 6

today, her odyssey is just beginning. As an adult Jehovah's Witness, she had the ethical duty to refuse blood products, as part of her religious convictions. In the setting of a 45 percent TBSA burn, though, such a conviction placed her at an extremely high risk of mortality. Because modern burn surgery relies on transfusion technology to facilitate wound excision and grafting, Maria was not a candidate for operative intervention and almost certain to have multiple complications, which she did: congestive heart failure, peridardial tamponade, profound anemia, deep venous thrombosis, pneumonia and burn wound infection.

As providers, we desperately recommended transfusion, but Maria exercised her right, her freedom, to choose against this intervention.

Maria had survived her resuscitation, but she was not prepared for what happened next. Slowly and insidiously, her burn wounds sloughed, giving way to painful, hypertrophic scars that covered her face, neck and hands. Her bone marrow shut down. Her liver became congested.

She then made a decision based upon the peculiarities and the particulars of the situation: she would receive some blood products – recombinant erythropoietin, albumin, clotting factors and xenogeneic blood substitutes – and this decision would be kept confidential, between provider and patient.

Maria is going home next week, and we are planning multiple reconstructive procedures, including laser therapies to ablate and resurface her scars. Maria made the decision to live, and an ethicist such as Dietrich Bonhoeffer would have smiled. PSN