"If you value your financial security, listen to this man."
—WILLIAM BRATTON, former police commissioner, NYPD and LAPD

SCAM ME IF YOU CAN

Simple Strategies to Outsmart Today's Rip-off Artists

EXCLUSIVE PREVIEW CHAPTER FOR AARP MEMBERS

FRANK W. ABAGNALE

author of #1 *New York Times* bestseller *CATCH ME IF YOU CAN*

Find this book at AARP.ORG/SCAMMEIFYOUCAN

SCAM ME IF YOU CAN

Simple Strategies to Outsmart Today's Rip-off Artists

FRANK ABAGNALE

PORTFOLIO | PENGUIN

AARP
Real Possibilities

4.

Sick: Medical Identity Theft

Personal data—containing everything a crook needs to commit financial identity theft, including your Social Security and financial account numbers—sells for about $25 on the black market, said Jon Ramsey, former chief technology officer of the Counter Threat Unit of SecureWorks and now CTO of the Counter Threat Unit of SecureWorks. But stolen health insurance and medical records can fetch far more: about $2,000 per person. That's because scammers use your information to submit fraudulent claims in your name to Medicare and other health insurers. The greater potential yield of medical identity theft—a $20,000 surgery, say—justifies the higher price. In this chapter we look at ways medical identity thieves can rack up bills, steal your identity, and disrupt and even harm your medical care. And, of course, I show you how to prevent that from happening.

In May 2018, Louisiana resident Heather Karpinsky and her family went on vacation. When they returned, Heather checked

Find this book at AARP.ORG/SCAMMEIFYOUCAN

the mail and noticed something unusual: the large amount of mail addressed to her five-year-old-son, Gavin. "I wondered why there were so many advertisements addressed to him, but I ripped them up and tossed them and didn't think much about it," recalled Heather. But the next day, Gavin received two more ads in the mail. She checked with her neighbor to see if her young children were also getting ads in the mail, but the neighbor said no. Then, two days later, Gavin received a collection notice in the mail. Inside was a bill for $200 for health and nutrition products bought through a television infomercial. Gavin didn't watch a lot of TV, and, being only five, he wasn't yet adept at ordering products over the telephone. And he certainly didn't have a credit card, though these orders had been placed with one.

Heather immediately called the credit card company, which determined that the bill was indeed fraudulent. Four days after she received that collection notice, her son's medical provider called to tell Heather its computer had been hacked, compromising the names, dates of birth, Social Security numbers, and insurance company information of fourteen minor patients of the office, including Gavin and his brother. His brother's information had not yet been used, but Gavin's information had been used to buy many over-the-counter health and nutrition products.

The only way for Heather to combat this scheme was to get Gavin fraud protection, which he will need for the rest of his life. "I was told his information will continue to be sold on the black market, and his medical identity can continue to be used," said Heather. Credit cards opened in Gavin's name also generated credit reports from the big three credit bureaus. "He's five—he shouldn't really have a credit report or a credit rating." But since he does, he also has credit monitoring. Heather will have to

Find this book at AARP.ORG/SCAMMEIFYOUCAN

monitor Gavin's credit until he is an adult, and then he will need to monitor it.

"Since Gavin's information was leaked, his insurance company, Blue Cross Blue Shield, has a new policy in place," explained Heather. "His account has been flagged as compromised, and if we receive any fraudulent charges for medical care, he is not liable for them. The bill goes back to the provider." When Gavin visits a new provider, Heather must present a photo ID. For now, it's Heather's driver's license, but when Gavin gets older, he will have to provide his own photo ID.

Heather did contact the police, who found that the doctor's office was not liable. The office had paid for a security system to handle its data, and that was where the breakdown had occurred. "Protecting your medical identity is a burden that falls on the victim," said Heather. She wonders how hard it will be for her son when he grows up and wants to use a credit card or needs to prove his medical identity to new doctors. For now, his credit is frozen—but his personal information and medical records are out there forever.

"I did not realize that this information was so valuable," said Gavin's mom. "I thought I was so careful. I never even wish a happy birthday to my boys on social media because I don't want to put that personal information into the public. Now I know that you're still vulnerable, even if you take precautions." Heather thought she was protecting her family, but she was powerless to stop her son's information from being stolen. We can't prevent data breaches, but we can take steps to protect ourselves.

Find this book at AARP.ORG/SCAMMEIFYOUCAN

MEDICAL IDENTITY THEFT HURTS

You want to protect yourself against medical identity theft because crooks can use your medical insurance or personal medical information to get treatment or medication, or to submit false billings in your name. Medical identity thieves can steal more than your insurance ID number—they can also rob you of your health. If someone gains access to your medical files or insurance card and uses them to get services, you might receive improper care because the thief's medical information can become mixed up with yours—and you could end up fighting a long battle with your provider for the bills an impostor racks up for prescriptions and health services, including expensive surgeries. The thief can also use this information to engage in nonmedical fraudulent activities.

Unlucky victims have been arrested and charged with drug crimes after an identity thief used their information to buy thousands of dollars' worth of opioids or other drugs with street value. One day, Deborah Ford, a retired postal worker from Houston, received an unsettling phone call, according to *Consumer Reports*. A bail bondsman told her she was going to be arrested for procuring more than 1,700 prescription opioid painkillers from a variety of local pharmacies. That call was *not* a scam, and she *was* arrested on drug charges. "I had my mug shot taken, my fingerprints taken," Ford told a reporter. She suffers from psoriasis, and the stress from being arrested led to a severe breakout. "The policemen looked at my hands and said, 'That's what drug users' hands look like.' They just assumed I was guilty."

What ultimately saved Deborah from being prosecuted and

Find this book at AARP.ORG/SCAMMEIFYOUCAN

convicted was a police report she had filed a couple of years earlier, after her purse was stolen from her car while she was inside a gas station. Ford did all the right things as soon as she discovered the theft: She filed a police report, canceled all her credit cards, obtained a new driver's license, and applied for and received a replacement health insurance card. After making sure none of her bank accounts had been compromised, she forgot about the incident. Life went on. Until that call from the bail bondsman.

The thief had altered Ford's driver's license, swapping out the photo but leaving her name and other identifying information. Then the thief used the license and her health insurance card to go to doctors to request prescription painkillers. One local pharmacist became suspicious about multiple prescriptions for a controlled substance and called the police, which led to Ford's eventual arrest. Even though the arrest was a mistake, it took seven years, from 2008 to 2015, for Deborah to clear her name.

SMART WAYS TO MINIMIZE THE RISK OF MEDICAL IDENTITY THEFT

You can't prevent data breaches or employee theft. But you can use these steps to spot problems and protect yourself.

- Monitor your bank and credit card accounts to check for medical costs you did not incur, especially if you've been notified of a breach of your medical information. Act promptly to correct the record. Report scams to your insurer and the three major credit-reporting firms—Equifax, Experian, and TransUnion.

Find this book at AARP.ORG/SCAMMEIFYOUCAN

- Read your "explanation of benefits" statements and your Medicare Summary Notices (received quarterly) thoroughly and carefully. This is the paperwork your health insurance company provides that shows the doctor visits, tests, and services the company has paid out for you. If you see a payment for a service you don't recognize, follow up on it immediately and persistently, until it is corrected or resolved. It could simply be a billing error, but it could also be an indication of attempted medical identity theft. This is often the only clue you get until the thief has made off with thousands—or hundreds of thousands—of dollars in medical services using your name. Read every letter from medical insurers and healthcare providers, including those that say "This is not a bill." If you see a doctor's name or treatment date that looks unfamiliar, speak up. And don't hesitate to ask someone you trust to look over this paperwork with you. Sometimes a second set of eyes will catch a suspicious charge you might have missed.
- Bring your Medicare or insurance card to the initial visit with a provider. After that, carry only a copy of the card, with all but the last four digits blacked out.
- Keep your medical bills, records, and any information with your insurance, Medicare, or account numbers in a safe place. If you do not need the information contained in these papers, use a micro-cut shredder to dispose of them—and that includes prescription drug labels and receipts.
- Unless you've placed the call, do not give out personal information over the phone about your healthcare or

Find this book at AARP.ORG/SCAMMEIFYOUCAN

health insurance. Do not respond to emails that ask you to give this information by return email.

- Be extremely skeptical of offers of "free" medical services. Be wary of giving your medical information to anyone promising you something for nothing.
- Avoid posting on social media about any surgery, medical procedure, or visit to a specialist. Medical identity thieves can appropriate the information to augment a false identity they assume with your credentials.
- Ask all your doctors to give you a copy of everything in your file (you may have to pay for copies) so you'll have a paper trail if needed.
- Avoid getting screenings (free or otherwise) at unfamiliar health fairs or storefronts that require your insurance information.
- Hang up on phone calls from people promising free supplies or asking for information about your health, healthcare, or health insurance.
- If you have a caregiver or housekeeper coming into your home, make sure to keep medication bottles locked up. With everyone carrying smartphones with cameras included, it's easy to snap a photo of the medication label to get a refill.

Find this book at AARP.ORG/SCAMMEIFYOUCAN

Hall of Shame: Yennier Capote Gonzalez

In August 2010, the Department of Health and Human Services got a tip that a man in Miami, Florida, had attempted to wire $17,000 from a newly opened Tennessee account to a Florida bank. That account had also recently received $38,000 from Medicare, according to a Department of Justice press release. Transactions of large sums of money often raise suspicions at banks, and in this case, the suspicions were justified. Yennier Capote Gonzalez had opened the account for his recently incorporated business, Gainesboro Ultimate Med Service, in a rural area of Gainesboro, Tennessee. But when law enforcement officials visited the property, it was pretty clear it wasn't a medical services company: The only structures on the property were an old barn and an uncompleted house.

The investigation that followed showed that Gainesboro Ultimate Med Service was a fake company and that, through it, Gonzalez had stolen the identity of a Knoxville, Tennessee, physician and used it to obtain a Medicare provider number. He then submitted claims under the guise of the phony company using the names of several Medicare beneficiaries who lived in South Florida—people who had also been victims of medical identity theft. These patients were billed for services purportedly rendered at Gainesboro Ultimate Med Service, even though they had never been to Tennessee.

In 2010, the U.S. government caught up with Gonzalez after he attempted another wire transfer. He was tried, sentenced to 67 months in federal prison, and ordered to pay restitution of $19,296 for his role in the fraudulent scheme.

Find this book at AARP.ORG/SCAMMEIFYOUCAN

MEDICAL RECORDS THEFT: WHAT HAS THE EXPERTS WORRIED

In November 2017, police in East Brunswick, New Jersey, got a call about a break-in at a storage facility. The burglars had methodically removed some thirteen boxes full of papers. This seemed like a peculiar heist. If thieves went to the trouble of breaking into a storage facility, wouldn't you think it would be to steal the jewelry, silver, or other valuables stored there? Did the criminals break into the wrong storage unit by mistake?

It turns out this was no run-of-the-mill theft. Inside the boxes were patient records from a medical practice, Otolaryngology Associates of Central Jersey, and those boxes full of paperwork were a bonanza for identity thieves. The records contained patients' names, addresses, phone numbers, dates of birth, medical histories, insurance and Medicare information, Social Security numbers, driver's licenses, and details of military service.

The street value for peddling this information meant a sweet payday for the crooks and endless headaches for the medical practice, which had to notify a thousand patients that their information had been compromised. After an intense investigation that involved not only the police but also the U.S. Department of Homeland Security and the Middlesex County Prosecutor's Office, arrests were made and the records were recovered before the majority of them were sold. One of the thieves was caught when he tried to sell an identity to someone who alerted authorities.

What makes this story unusual is, first, that it was an old-fashioned burglary of actual paper files and, second, that justice

Find this book at AARP.ORG/SCAMMEIFYOUCAN

was swift and the perpetrators caught. Identity theft from large medical organizations is usually done by hackers who steal digital files. These thieves are rarely identified or caught, because they do not leave a "digital fingerprint," or they are overseas and beyond the reach of domestic law enforcement. In fact, one of the major factors behind the increase in medical breaches and theft is that medical records today are predominantly digitized. "Digitized records are much easier to steal than paper ones," Deborah Peel, a physician and founder of Patient Privacy Rights, a nonprofit advocacy group in Austin, Texas, told MarketWatch. Digital medical records are also often stored in millions of databases, which makes correcting them after they've been altered by thieves incredibly difficult, said Peel.

Data breaches cost the healthcare industry more than $6 *billion* annually, according to the Ponemon Institute. Often officials who oversee hacking thefts have a hard time determining whether anyone's information was actually used. Some twenty-seven million individual medical records are stolen each year. In 2017 alone, 477 healthcare data breaches were reported to the U.S. Department of Health and Human Services or the media, which affected about 5.6 million patient records, according to Protenus, a company that tracks healthcare industry breaches. Some experts even predict that by 2024, all people living in the United States will have been part of a health records data breach!

Most data breaches in the healthcare industry are actually inside jobs. As I warn my corporate clients time and again, *data breaches don't happen by themselves*. A crooked or disgruntled employee can pilfer information from a single file or files, or simply remove an entire filing system. But employees don't have

Find this book at AARP.ORG/SCAMMEIFYOUCAN

to be angry or greedy to cause a data breach. They can simply be careless.

The major reasons for data breaches in medicine are different from those in other industries, according to a 2018 study by Verizon, "Protected Health Information Data Breach Report." According to the report, 35 percent of digital breaches are caused by human error, including misdelivery of information, disposal mistakes, and loss. More than 16 percent of breaches are caused by internal theft of information. Not securing a password, leaving a device where it can be stolen, or failing to update software with a security patch can lead to data breach. Security procedures are only as good as the people who implement, maintain, and monitor them. A slip-up at any point in that process leaves an opening for a data thief to take advantage of.

And take advantage they will. Even if they don't have an unwitting "accomplice" like a careless employee making it easy for them to get into a company's records, data criminals have other means of stealing medical information. Malware, denial-of-service (DoS) attacks, and ransomware are all ways to obtain information illegally. In some instances, companies whose data has been snatched by these methods don't even know it.

MEDICARE RECIPIENTS ARE ESPECIALLY VULNERABLE

Many of us acknowledge turning sixty-five with mixed feelings. I know I did. But I was (and am!) thrilled to reap one reward of that milestone: my Medicare card. I was less than thrilled,

Find this book at AARP.ORG/SCAMMEIFYOUCAN

however, when I saw my Social Security number emblazoned across the card, for any and all to see, copy down, and claim. If you have received Medicare for a while, you've probably noticed the same thing on your card.

It wasn't until 2015 that the government passed a law requiring that Medicare and Social Security numbers be different—something I lobbied hard for, as did AARP. Since April 2018, the Centers for Medicare and Medicaid Services of the Department of Health and Human Services, which administers Medicare, has been rolling out its replacement card program. New Medicare cards bearing a new identification number—*not* your Social Security number—are being sent to all Medicare recipients on a state-by-state basis. If you're on Medicare, you should have yours by now. There is no question that having two different numbers dramatically reduces the threat of identity theft from a lost or stolen Medicare card. That's the good news.

The bad news is that the longtime use of your Social Security number for Medicare has spawned more than a few organized efforts by scammers to trick Medicare recipients into giving away their Social Security number. Some scammers will call you, spoofing the caller ID so it looks as if they're calling from Medicare. They'll ask you to pay a processing fee to receive your new card. Or they'll say they need to verify your Social Security number in order to send your new one. This is fraud. The cards are free, and Medicare would not call you to verify your Social Security number—the administration already has it.

Find this book at AARP.ORG/SCAMMEIFYOUCAN

RESOURCES: MEDICARE IDENTITY THEFT

If you receive Medicare and think that you have been a victim of medical identity theft, you have dedicated resources available.

- Report suspicious calls regarding your healthcare or health insurance to 800-MEDICARE (800-633-4227).
- Each state has a Senior Medicare Patrol (SMP) that can give you reliable information and help with all your Medicare questions, including those about possible fraud or identity theft. You can locate your state's office at www.smpresource.org/content/what-smps-do.aspx. Staff here will also help you determine whether fraud or theft has occurred.
- If you have established that someone else is using your Medicare benefits, follow the same procedure as with any other kind of identity theft and begin by making a report at identitytheft.gov.

MEDICAL RECORDS THEFT: WHAT CAN BE DONE TO STOP IT?

We're a long way from eliminating the threat of medical identity theft through cybercrime, but I see some hopeful signs of improvements. First, the industry itself is more aware of the problem than ever before, due to the high-profile nature of breaches. For

Find this book at AARP.ORG/SCAMMEIFYOUCAN

example, in 2017 a breach caused by a ransomware virus left information from more than 266,000 patients vulnerable at the Pacific Alliance Medical Center, in Los Angeles. The hospital's IT staff had to scramble to figure out how to deactivate the virus before re-encrypting the vulnerable files. We don't know if the hospital paid a ransom to the criminals. We do know that it notified the patients affected and offered to pay for two years of credit monitoring for them. Two years is not long enough, in my experience. Criminals are patient and have been known to wait five years or more to use stolen information, so credit monitoring and ID protection need to be done long-term. Any credit-monitoring service you use should look at the big three credit bureaus (Equifax, Experian, and TransUnion) and give you real-time notifications of any breaches.

Businesses that work with medical records should take action to heighten the security of those files. As a consumer of the services these businesses provide, I check to see if they have certain policies and procedures in place. I recommend you ask these questions as well; they should become part of how you advocate for yourself with your providers. After all, the accuracy and safety of your medical information is crucial for receiving the best and most appropriate care. I ask:

- Are employees trained in the correct procedures for safeguarding data? Training should be frequent and updated as new threats appear and new solutions are identified. Proper data security should be an integral requirement of every job that requires employee access to data, and employees should be evaluated on these criteria.

Find this book at AARP.ORG/SCAMMEIFYOUCAN

- Is employees' access to secure data limited through the use of passwords as well as the devices that can connect to the information? Portable devices such as tablets, smartphones, and laptops are easily lost or stolen—and can be left in a place where an unauthorized user can help himself to information.
- Does the business have a recovery plan in place, one that is reviewed and updated frequently, spelling out the actions to take in the event of a data breach, including a plan to help patients recover and correct their medical records?
- In the event of a data breach, does the business offer affected patients a minimum of three years or, ideally, at least five years of identity theft protection?
- Is the business insured against data breaches? If one happens, are there funds available to investigate the crime, fix the vulnerability in the system, and assist victims with the damage done to their lives and reputations?

MEDICAL RECORDS THEFT: WHERE DO WE GO FROM HERE?

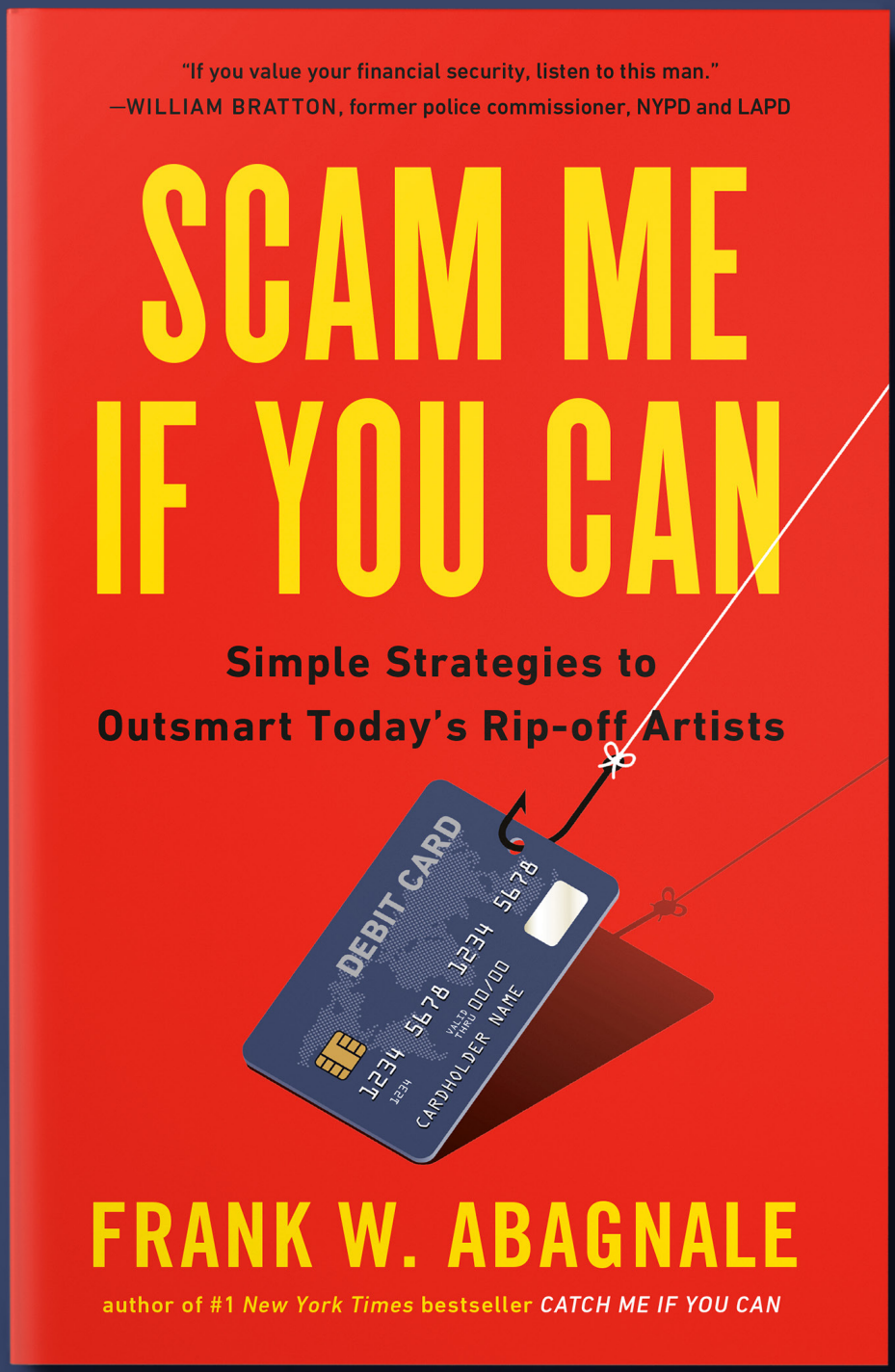
Awareness is the best place to start, and businesses are paying more attention by looking for vulnerabilities in their computer systems, running mock scenarios, and holding employees to higher standards of accountability. The government has taken a major step by changing Medicare numbers so they're different from our Social Security numbers. We may want to see if legislation

Find this book at AARP.ORG/SCAMMEIFYOUCAN

recently enacted by the European Union, called the General Data Protection Regulation, is effective in limiting data theft of personal information. It's a complex law, but one of its key provisions, called pseudonymization, replaces identifying information about you with random codes or "pseudonyms." That means that anyone working with the information—employees or thieves—would not be able to identify the individual it belongs to. It can be used in conjunction with encryption for an extra layer of protection. A special digital key is required to match the code with the information. It's a start, but as of this writing, pseudonymization is not widely used in the United States. So for now we must remain vigilant when it comes to the valuable commodity that is our medical identities.

BUY THIS BOOK NOW

- AMAZON
- BARNES AND NOBLE
- INDIEBOUND
- APPLE BOOKS



AARP® Real Possibilities

PORTFOLIO PENGUIN