



## Debt Tagging:

### When you get tagged with someone else's debt

Every morning, Michael Brown practices yoga for two hours to stay physically and mentally limber. But when debt collectors mistook him for an M. Brown who owed \$1,000 in medical bills, not even his yogi discipline could prepare him for the fight for his identity.

**Debt Tagging** occurs when collectors target the wrong person for a debt. Identity Theft 911's fraud resolution center dubbed the practice "tagging" two months ago after a spike in these types of cases.

Over an 18-month period, Brown endured hundreds of abusive phone calls—sometimes as many as four a day. He says his perfect credit plummeted and his credit card interest rates tripled because the debt was placed on his credit report. And when he couldn't secure a loan to repair a tool needed for his sign-making company, he was forced to go out of business.

"They cost me thousands of dollars, harassed me for a year and a half, and destroyed my business," said Brown, 46. "If I even see an unknown phone number (calling), my stomach starts twisting."

[Continued on page 3](#) ▶

## The Vultures of Summer: Identity crooks want to ruin your vacation—don't let them

Summer vacation season is almost here, and fraudsters are counting on travelers to be carefree, and a little careless, when away from home.

They're ready to strike at restaurants, hotels, gas stations, Internet cafes, and car and recreation-equipment rental locations. That's because tourist destinations are notoriously easy hunting grounds for criminals—both old-school purse-snatchers and a new breed of sophisticated hackers. And though part of getting away means relaxing, experts say the key to avoiding a vacation nightmare is to be aware of the latest crime trends and to never let your guard down. [Continued on page 5](#) ▶



It's hard to imagine a world without Google, Facebook, or the many technological innovations we now accept as part of our daily routine: Our phones are smarter, our computers more portable, our opportunities to share information with a worldwide audience unprecedented. The changes are big and exciting. And yet, they arrive without us having had time to step back and fully evaluate how this shift in social and professional activity might be reconciled with the age-old value we place on privacy—from a policy, business and consumer perspective.

These days, there are new versions of malware, new sources of data compromise, and emerging threats with more overtly political implications—like the hacking of Yahoo e-mail accounts belonging to journalists, scholars and activists in China. All of this means our privacy is continually being eroded.

But the good news is that we're meeting these threats with newfound organization. Just as the Green Movement was strengthened and brought into sharper focus as a result of growing environmental concerns, so too is a privacy movement gaining traction in the face of new challenges.

In this month's newsletter, we talk to Identity Theft 911's chief privacy officer, Eduard Goodman, about how different governments worldwide have addressed this increasingly important issue, and why there are unique rifts between how Europeans and Americans approach privacy. We offer stories on what to do when debt collectors have mistakenly targeted you for someone else's debt, how to stay safe on vacation, and the dangers of sharing Social Security numbers for small business tax purposes.

As always, we hope you'll enjoy.



Matt Cullina  
Chief Executive Officer,  
Identity Theft 911

## In this issue...

### FEATURES



- 4 Small Business:** A daycare provider learns—the hard way—the importance of using an Employment Identification Number, instead of her Social Security number.

### DEPARTMENTS

- 6 Case Study:** June Smith shares lessons learned from her four-year battle against medical identity theft.
- 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 Chief Privacy Officer Eduard Goodman sheds light on Google's privacy battles in Europe.

In the past two months, the Identity Theft 911 Fraud Resolution Center has experienced a spike in cases that involve “debt tagging”—when debt collectors target the wrong person for a debt. These cases exact a toll on victims, particularly in the wake of the financial crisis, by damaging credit and taking months to resolve.

Complaints against third-party debt collectors increased by 10 percent in 2009 from the previous year, according to April’s Federal Trade Commission report on the Fair Debt Collection Practices Act. (Third-party debt collectors include contingency fee collectors, attorneys who regularly collect, and debt buyers collecting on debts they purchased in default.) And they were the second-most common complaint, behind identity theft, in the FTC’s Top Consumer Complaints of 2009.

Other common grievances against collectors: harassing or threatening behavior, trying to collect more than was owed, and failing to send required notices to consumers.

In March, a national debt collector agreed to pay a civil fine of more than \$1 million to settle FTC charges that it violated federal law by inaccurately reporting credit information and pressing consumers to pay debts they didn’t owe. Credit Bureau Collection Services, based in Columbus, Ohio, illegally tried to collect invalid debts, reported them to credit reporting agencies without noting consumers had disputed them, and continued to assert consumers owed debt even after the debt had been paid or clearly didn’t belong to the consumer.

The major cause of “wrong party contacts,” as debt tagging is referred to in the debt collection industry, is the portability of phone numbers, said Valerie Hayes, general counsel for ACA International, the collectors’ trade group. “It isn’t that you’ve been a victim of

identity theft or something nefarious,” she said. “It’s because someone gave up their number and it’s been automatically assigned to someone new.”

It’s also difficult for debt collectors to identify the correct debtor when consumers have common names such as Joe Smith or Michael Brown, she said. Mistakes can happen during the “skiptracing” process, when collectors try to locate a person’s whereabouts by contacting phone number databases, credit reports, job application information and a number of other resources.

The problems caused by a lack of information available to debt collectors prompted the U.S. Government Accountability Office to call for major changes to the Fair Debt Collection Practices Act in a report released last October. The report said poor information sometimes leads “the collector to try to collect from the wrong consumer or for the wrong amount” because he “may not have access to billing statements or other documentation needed to verify the debt.”

The GAO report also noted that as the prevalence of debt-buying increases—when collectors sell and resell debt bundles for a fraction of their original value—it becomes more difficult to verify debt as it moves further away from the original owner.

“There are no requirements that debt collectors verify they have the right person before they place the debt on a credit report,” says Gerri Detweiler, a personal finance expert for Credit.com and co-author of *Debt Collection Answers: How To Use Debt Collection Laws To Protect Your Rights*. “So it can be pretty easy to end up with someone’s debt.”

It’s a frustrating reality for victims like Brown, who spent hours on the phone with credit bureaus and endured abusive phone calls from collectors unwilling to accept his written and verbal insistence that they had the wrong guy.

One side benefit? It’s helped his yoga.

“The last year has been great for my yoga practice, and there’s a connection, without a doubt,” Brown said. “It’s easier for me to be focus on the present when things are really crazy around me.” ■

## What To Do When When You’ve Been Tagged

1. When a debt collector first calls, ask him to send a written notice within five business days, which he’s required to do by law.
2. If you don’t owe the debt, tell the collector he’s got the wrong person. Ask for the collector’s mailing address. Send a letter restating that he’s got the wrong person and ask him to stop contacting you.
3. Track any subsequent calls from collector.
4. If verbal and written communication doesn’t work, contact ACA International at (952) 926-6547. The collectors’ industry trade group can work to resolve problem through its ethics department.
5. File a complaint with the Federal Trade Commission against aggressive collectors by visiting [ftc.gov](http://ftc.gov) or calling 1-877-FTC-HELP (1-877-382-4357).
6. Check your credit reports on [annualcreditreport.com](http://annualcreditreport.com), a government-approved source for free credit reporting information, to make sure the debt hasn’t been mistakenly attached to your report.

# Don't Leave Your Small Business Exposed:

## Use of SSN for taxes heightens risk

For Rebecca, a small town had its advantages. She was on a first-name basis with her bank. Neighbors treated her as family—a daycare provider for the past 38 years, she had, in fact, looked after many of them or their children.

So at year's end, as clients were collecting information needed for tax write-offs, she didn't think twice about giving them her Social Security number, which she'd always used to identify her home-run business to the Internal Revenue Service. That is, until she received a letter from the agency at the beginning of March.

"It said my federal income tax didn't jibe with the one from last year," explains Rebecca. (We aren't using her real name to protect her privacy.) The amount she'd reportedly claimed as her refund—10 times higher than what she was actually owed—raised a red flag with the IRS. The agency's letter raised an even bigger red flag with Rebecca: She hadn't yet filed her 2009 taxes. "It just didn't make sense," she explains. "(Someone who had already filed) had my name, my address, and my Social Security number."

**"It said my federal income tax didn't jibe with the one from last year." "It just didn't make sense." (Someone who had already filed) had my name, my address, and my Social Security number." — Rebecca**

It's not the first time an unauthorized individual has tried to file a fraudulent return in somebody else's name. Last year, a U.S. Government Accountability Office (GAO) report pointed to more than 23,000 such incidents through Dec. 31, 2008. (In only 10 percent of the incidents did the scammers actually succeed in making off with government cash.)

Alarmed, Rebecca started making calls. She and her tax preparer began working with an IRS fraud specialist. But with her SSN out there, there was a risk it might be misused for purposes other than tax fraud—namely, credit card fraud or the opening of other unauthorized credit accounts. Her bank put her in touch with Identity Theft 911 fraud resolution specialist Omar

Edwards, who helped her through the process of filing a police report, putting fraud alerts on her credit file, reviewing her credit reports for signs of fraud and more.

So far, there's been no sign of additional compromise. And, as is the case with many identity theft cases, no one can determine exactly the source of her Social Security number exposure, Edwards says. Handing an SSN out for tax purposes, however, unnecessarily adds to the risk faced by small businesses, says Identity Theft 911 Chief Privacy Officer Eduard Goodman.

Instead, small business owners ought to set up an Employer Identification Number. "It's very easy to file," Goodman says. "The average person doesn't need a lawyer."

Individuals should check with their state for specific requirements; the IRS offers an application process online. Using an Employer Identification Number limits SSN exposure, and makes business and personal sense, Goodman says.

Going forward, Rebecca says, she'll be using the EIN in lieu of her Social Security number. "That was really scary. I don't wish it on anybody," Rebecca says of her ordeal. "I'm the kind of person that likes to have everything right." ■

“Basically, what you’re looking at here is you’re looking at the potential of being ripped off in a variety of ways,” says Jay Foley, executive director of the Identity Theft Resource Center, a non-profit based in San Diego. “(Using) the wireless from the hotel. Cards cloned from the hotel. Personal information lifted from the hotel. Someone cleaning your room—and you don’t have any idea who they are.”

The main spot where travelers are most vulnerable? Their hotel. Theft not only happens in rooms and lobbies, but on hotels’ computerized payment systems.

Hackers steal credit card data from hotels more than any other industry, according to a February report by cybersecurity firm Trustwave. Some 38 percent of the company’s data breach investigations in 2009 occurred at hotels, compared with a distant second place of 19 percent for financial services firms. That’s a significant increase in hotel hacking from the year before, Trustwave officials said.

The report noted that it took a jaw-dropping average of 156 days for a business to realize it had been hacked.

Travelers become vulnerable the moment they give their credit card to the hotel for more basic reasons. Suddenly, every employee in the hotel may have access to the guest’s information.

In hotel bars and restaurants, be on the lookout for skimmers. Someone—maybe a waiter or someone distracting the waiter collecting a credit or debit card for a dinner bill—can take it and quickly run it through a small data storage device. The card’s information has been loaded onto the device. The perpetrators can download the information later to make a brand new card, or several, which can be used around the country before the fraud is discovered.

Mark Fullbright, a fraud specialist with Identity Theft 911, says gas stations and services near hotels are another prime spot for skimming—often done by the low-paid employees of the businesses. The skimmers know many customers are likely to be travelers, who may be leaving town soon and unable to file police reports. And it may take weeks or more before they even discover the fraud.

**“Basically, what you’re looking at here is the potential of being ripped off in a variety of ways.”**

*— Jay Foley, executive director  
of the Identity Theft Resource Center*

But there are ways to make it harder for thieves to access your personal information, experts say.

Try to carry a PIN-based ATM card, which requires entering a PIN number with every purchase, instead of a debit card. Bring two credit cards, and watch all card activity closely (checking accounts by phone or a secure computer, if possible) for any unauthorized charges.

Avoid accessing personal accounts on public computers. They’re a common source of identity theft because they have a high volume of usage on unprotected signals. And be wary of people hovering near you. They may be using cell phones to photograph your personal information.

“Being a little prepared . . . lets you have a better trip altogether,” Fullbright says. ■

## Tips for a fun—and safe—family vacation

1. Use a PIN-based ATM card instead of a debit card.
2. Leave your checkbook, debit card and all but two credit cards at home.
3. Closely watch who has your credit cards and for how long. Frequently check credit card and bank account activity on a secure computer or by phone.
4. Tell your banks and credit card companies about your travel plans, and give them your cell phone number in case they notice unusual charges.
5. Don’t access personal or financial information on public computers, and make sure, when using your own laptop, that the wireless system you’re using is legitimate and secure.
6. Use a hotel safe when available. Your hotel is not your castle. Assume your locked door will never be truly “locked.” Many people you don’t know will have access to your room.
7. Never leave personal information in a rental car.
8. Never share specific vacation plans on social networking sites.

## Case Study: Medical Identity Theft

June Smith had a funny feeling the medical charges were fraudulent. The 72-year-old New Yorker's first clue? The bill for a pregnancy test.

Beginning in 2006, Smith's personal information—including her Social Security number—was used to charge Medicare for tens of thousands of dollars of medical services in her name. Despite her attempt to alert officials, she says, Medicare paid the bills. Though Smith and her husband, Thomas, didn't incur any personal charges from the fraud, they worried they'd reach a Medicare benefits cap and ultimately be denied legitimate services they might need in the future.

The Smith case illustrates the challenges many victims of medical identity theft face—often when they're at their most vulnerable due to age, infirmity or limited resources in retirement.

"It's important for people like me to have their eyes open," Smith says. She hopes her story, recently featured on WABC-TV's "7 on Your Side," offers a valuable lesson for other potential victims.

Medical identity theft begins when someone gains access to a victim's personal information. A fraudster can rack up medical charges very quickly. And those charges can cost insurance companies, Medicare, and victims—through assessed co-pays for services never received.

It's often difficult to untangle what has happened, and to get medical providers and insurance companies to understand that a fraud has taken place.

"Why are you paying these bills?" Smith once asked a Medicare representative, after explaining her situation. The rep responded, according to Smith: "Because they come to us."

**"It was just a sigh of relief. After years of her complaints falling on deaf ears, they were starting look into whatever the complaints were and (understand) that she may be right."** — Mark Fullbright *Identity Theft 911 Fraud Specialist*

Through her homeowners insurance, Smith reached Identity Theft 911 fraud specialist Mark Fullbright. After an investigation, he discovered that many of the supposed doctors and medical entities making the charges weren't licensed as physicians or operating as legitimate businesses. They appeared to be fictitious people and institutions created by scammers who were still receiving very large checks.

Fullbright detailed those particulars in letters he wrote to various authorities, including Medicare officials. And while he never got direct responses, Smith finally received a letter from Medicare last year. The letter stated that one group of charges were considered fraudulent and would not be paid. Medicare was finally paying attention to what she says she had been saying for years.

"It was just a sigh of relief," Fullbright says of that first acknowledgment. "After years of her complaints falling on deaf ears, they were starting look into whatever the complaints were and (understand) that she may be right."

Four years after the first suspicious bills, Smith's ordeal isn't over. She still gets notices of charges to Medicare that are obviously wrong. But Medicare has stopped paying them. ■

## Hits



If a careless retailer loses customer payment card data, should banks and credit unions bear the expense of issuing new cards? Not in the state of Washington. Following on the heels of a similar Minnesota law, a new law in Washington allows financial institutions to recover such costs if a business fails to take reasonable measures to protect sensitive data. One caveat: A business won't be held liable if it can demonstrate that it meets the PCI-DSS, or payment card industry security standard, within one year prior to the breach.



Suspects who are accused of filing more than 1,900 fraudulent tax returns (many using dead people's personal information) and making off with \$4 million of government money may see their alleged three-year run with identity theft come to a screeching legal halt. According to a 74-count indictment recently unsealed in Arizona, members of the group now face charges including identity theft, wire fraud and mail fraud. "While schemes become more sophisticated over time, fortunately so do our investigative techniques," said Dawn Mertz, special agent in charge of the IRS Criminal Investigation division, one of several federal agencies involved in the case.

## Misses



You'd like to think you can trust your tax preparer. But at least two customers of an H&R Block in the Bronx do not—and they've filed a class-action lawsuit to prove it. According to *The New York Times*, lawyers for Sharon Hawa and Kevin Johns have filed the suit alleging that, in the wake of IRS fraud incidents involving the customers' data, the company failed "to take steps to protect its customers' security despite previous allegations (and lawsuits filed in Arizona, Illinois and Michigan) against other H&R Block outlets."



Let's hope the news from the U.S. Government Accountability Office is a little better the next time around—at least as it pertains to federal agency data security standards. According to separate GAO reports issued in April, no federal agency has satisfied all the requirements of two key cyber-security strategies: the Trusted Internet Connection (TIC) or the Federal Desktop Core Configuration (FDCC) initiatives.



## Q&A: Eduard Goodman

### Lessons From Google's Privacy Battles in Europe

Google has come under fire for its privacy practices in Europe. In April, 10 foreign privacy commissioners criticized the Internet search giant for failing to protect user privacy. They cited the Google Buzz social network, which exposed users' Gmail contacts, and Google Street View, a mapping tool that shows photos of street scenes. In Italy, three Google executives have been convicted of violating privacy laws. Eduard Goodman, Identity Theft 911's chief privacy officer, addressed the subject at the International Association of Privacy Professionals conference last month. He attributes Google's problems to historically different approaches to privacy in the United States and European Union.

#### What's the perception of regional differences in privacy approaches for consumers in the E.U. and U.S.?

The perception is that the E.U. as a whole, and the 27 member nations that make it up, are more cognizant of your average consumer's privacy than here in the States.

#### Can you walk us through the history behind that perception?

In 1995, the E.U. passed the Data Protection Directive (95/46/EC), which addresses the protection of personal data. It required member states to bring national laws into line with one another regarding privacy and broadly covers all industry sectors. By comparison, U.S. privacy laws are considered "sector specific," meaning that specific pieces of regulation relate to specific areas, including credit transactions, video rental privacy and health care privacy.

While Europe got kudos for ensuring a baseline of consumer-oriented protection, the reality was that it was really commerce driven. The concern being that if the E.U. didn't issue the directive, some member countries with more relaxed privacy laws would have advantages over other members with stricter consumer-oriented regimes.

#### Does the E.U. offer its consumers better privacy protection than the U.S.?

It's not better or worse; it's different. In the U.S., we've put the cart before the horse by focusing on notifying consumers after a breach has occurred as opposed to securing the information.

The interesting thing is that now both regions are starting to look and learn from the other. In the U.S., we're taking a more European approach to protecting information before a breach or identity theft happens. Most of the progress has been on the state level. While 46 states now have breach

notification statutes, states like Massachusetts, Washington, Wisconsin, and Nevada, have gone further, asking "What do companies need to do to protect the data?" and have thus passed encryption, PCI security and other prescriptive security statutes.

Meanwhile, European nations are adopting U.S.-style breach notification laws, with the United Kingdom leading the charge.

#### How do the two regions differ in their approach to enforcing privacy laws?

Most foreign countries have a privacy commissioner or some equivalent to that position. We don't. That role has fallen to the Federal Trade Commission, which has a good, 10-year track record of enforcement. And it all comes down to what it considers deceptive and fair trade practices.

When you weigh the FTC against foreign privacy commissioners, the FTC actually has done a very good job of enforcing privacy violations by not just fining institutions that violate industry privacy and security "best practices" but by going further and often requiring regular outside audits, often times for up to 20 years, of these companies.

#### What message does Google's struggle abroad send to other companies?

Europe's approach to privacy is a bit overzealous in that it is a fine line between protecting consumer privacy and stifling the development of e-commerce. The positive aspect to a less rigid privacy regime in the U.S. is that it fosters companies like Google, Facebook, PayPal, and eBay. Europe hasn't completely missed out but because of its stifling privacy environment, it hasn't been able to incubate the innovative fast-growing companies like the U.S. has. ■