



NEWSLETTER

Identity Theft 911®

VOLUME 6

ISSUE 1

FEBRUARY

2009

AMERICA'S LEADING IDENTITY MANAGEMENT AND EDUCATION SOURCE

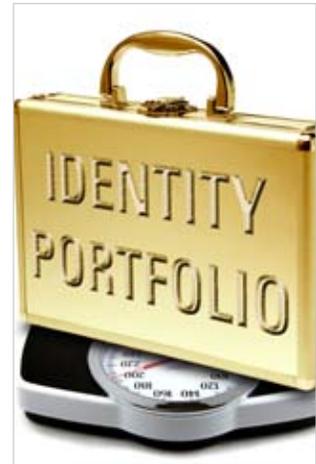
THIS MONTH'S TOPIC ...

New Year, New Threats

A New Weapon: Managing Your Identity Portfolio

Identity theft is never a welcome occurrence, but in a dismal economy, victims stand to suffer even greater devastation from the crime. Many now find themselves in a financial house of cards in which a single monetary lapse can bring everything crashing down. And when financial ruin comes at the predatory actions of an identity thief, it cuts even closer to the bone. Consumers must be mindful of the very real and ever-growing threat of the crime, and in doing so, they must get serious about mitigating the risks.

This is why it's vitally important to know the identity theft landscape. This month, we take a look back at the trends of 2008, and forecast the growing threats for 2009. Beyond that, we present a new mindset – a paradigm shift – if you want to gain greater control over your identity, you must manage it as you would your financial portfolio. It's as simple as that. What better time, while in the spirit of the New Year, to take stock and better secure your identity.



For a complete newsletter archive, visit: www.identitytheft911.org/newsletters

To learn about the latest scams on identity theft, visit: www.identitytheft911.org

Comments, questions? Contact us: newsletter@identitytheft911.com



Looking back

Every year we take stock, it appears that the previous year was good for identity thieves—2008 is, unfortunately, no exception. More Americans are estimated to have become victims of identity theft last year than ever before. More consumers had private data exposed in potentially dangerous security breaches. Scammers adopted powerful new technological methods, and they responded quickly to the deepening economic crisis by creating cons that prey on Americans' newfound financial insecurity. It was a deluge—an identity theft whirlwind that left consumers scrambling to pick up the pieces.

The silver lining? If any is to be found, it is in the tightening of restrictions surrounding how financial institutions grant credit and the approval of state-level measures intended to mitigate identity-related problems.

As the New Year continues, let's pause to reflect on the most important trends and biggest news events of 2008.

The Year in Review

Trends of 2008:

Identity Theft Still Growing Fast

Identity theft is rampant and spreading, according to the Federal Trade Commission, which found that 8.3 million Americans had their identities stolen in 2005, the latest year for which data is available. Since then, identity theft has remained the fastest-growing type of fraud in the country, the FTC has found. Even more people were placed at risk last year. Thanks to organizational security breaches, at least 35.7 million records were made susceptible to identity theft in 2008, according to the Identity Theft Resource Center (ITRC). And that represents only reported breaches. About 40 percent of breaches are never reported at all, partly because of lax corporate social responsibility: some businesses report them, and some do not. That means the actual number of potential victims exposed last year could be around 61.4 million.

“Most people believe identity theft has to do with check fraud,” Linda Foley, co-founder of ITRC, said recently in an interview with a banking industry trade journal. “But it goes far beyond that. We have younger thieves. We have people who are targeting specific populations, the elderly, children, critically ill patients, those who speak limited English.”

Online Thieves Get Serious

At the dawn of the information age, computer hackers were breaking into secured networks just for kicks and bragging rights. That began to change around 2001 and the pursuit of crime online has grown steadily ever since, and in 2008 more hackers officially went pro. They were emboldened by black market entrepreneurs, often funded by Russian mafia leaders, who last year launched a raft of new, underground software companies. Similar to their above-ground counterparts like Microsoft, these enterprises build and sell entire suites of software. The suites are loaded with many different malware programs that buyers can switch off or on at will. Thanks partly to these mega-Trojan packages, the number of malware programs released

on the web grew to almost half a million per month in 2008, according to Prevx, a Derby, England-based internet security research company.

“In addition to the exponential increase in malware volumes, Prevx researchers have seen a huge increase in highly targeted criminal software, like the PRG Trojan, which hijacks a consumer’s online banking session to steal from high-value personal and business bank accounts,” said Jacques Erasmus, a former hacker who now directs malware research for Prevx.

These professional hackers have proven themselves capable of stealing information anywhere, from simple targets like small New England towns to large corporations with top-notch computer defenses. In most attacks, the thieves are looking for financial information, especially credit card numbers, which can easily be used to steal cash, according to a report on the underground online economy released recently by the security firm Symantec.

With so much private financial data available for sale, the price of programs designed to steal it is soaring. During three months in summer 2008, identity thieves advertised \$276 million worth of malware programs and stolen data online, Symantec found.

“The online underground economy has matured into an efficient global marketplace in which stolen goods and fraud-related services worth billions of dollars are regularly bought and sold,” Wendell Davis, a spokesman for Symantec, said in a recent podcast.

Real Estate Down, But Not Fraud

Fraud provided the kindling that eventually resulted in economic meltdown. But as the FBI learned this year, identity thieves can game the real estate markets even in a bear market.

“Mortgage fraud is still happening,” David Morgan, the FBI agent who leads the bureau’s anti-mortgage fraud team in Cleveland, Ohio, told us last fall. “It’s big business.”

During the housing bubble, false identities were valuable because they could be used as “straw buyers” to extract real loans from banks, Morgan explained. (A straw buyer is a person whose credit

is used to secure a loan application, even though that person never intends to live in or control a property.) In the wake of the economic crash, stolen identities are still a hot commodity, as banks suddenly are left holding the deeds to tens of thousands of foreclosed properties and looking for quick sales. In their desperation, some are selling to buyers who suspiciously offer to pay above the asking price for houses or condos that have sat empty on the market for months, says Todd Lackner, a mortgage fraud expert in San Diego.

That often sets the stage for an even bigger scam, in which straw buyers using stolen identities obtain loans to buy nearby properties at inflated prices, only to walk away from the payments and steal the loan money.

“As financial institutions begin to enforce higher lending standards, the identities of individuals with good credit will increase in value to perpetrators” of fraud, the FBI said in a report this year. “As such, individuals with good credit will likely be at a more significant risk for identity theft and mortgage fraud schemes, and the continued vulnerability of identifying information will allow perpetrators the accesses necessary to commit such schemes.”

Big Institutions Woke Up (rather like Rip van Winkle)

In 2008, more business, government and educational institutions woke up to the threat of identity theft. One of the quieter—but perhaps most important—developments in this arena was the announcement by the Federal Trade Commission that it would *finally* pass the long-debated “Red Flag Rules.” Set to take effect in May 2009, after an overwhelming response that businesses ignored or weren’t prepared for the original November 2008 date, these regulations require financial institutions and creditors to protect consumers’ confidential information by identifying warning signs (“red flags”) that may indicate someone is trying to steal private identity information. If a red flag is raised, companies must investigate the problem, and take steps to ensure that all information is secure.

Other sectors are waking up to

the threat of identity theft, too. Schools and universities continued to improve their control over sensitive data in 2008. Learning institutions accounted for 20 percent of all security breaches reported last year, down from 28 percent in 2006, according to ITRC.

Breaches were more common at corporations, which accounted for 36 percent of information leaks in 2008, up from 21 percent three years ago. And more of those cases resulted from theft, as opposed to incompetence or absent-minded loss of laptops. The proportion of data leaks attributable to theft by “insiders,” current and former employees, grew from 7 percent in 2007 to 15 percent in 2008, ITRC found.

The good news? Anecdotal evidence that in 2008, businesses appeared to become more aware that they face a true identity theft problem. But awareness is one first step.

“We recently had a mid-sized institution in the U.S. that wanted to do a test of technology to help them monitor employee activities, and that ended up with two employees being arrested,” Amir Orad, chief marketing officer for Actimize, a fraud prevention company in New York, told the *Washington Post* in January. “That’s the type of outcome we did not see two years ago.”

With businesses on the slow end of the curve in implementing proactive safeguards and demonstrating greater responsibility, they face the added challenge of identity thieves picking up seed and getting more sophisticated. The race is on.

Major News Events of 2008:

The Economic Crisis.

For identity thieves, the sinking economy is the gift that will keep on giving, probably for years. Con men who made a killing during the real estate boom buying and selling houses using stolen identities quickly figured out a new scam: Posing as foreclosure “counselors” for families about to lose their homes. Using a small advance of cash to help the family make the next mortgage payment, these thieves charge exorbitant interest to force the homeowner to miss payments and go into default, which allows the crooks to

steal the house outright. “This type of fraud went from almost nothing last year to being the most common thing we see,” says Robert Strupp, director of research and policy for the Community Law Center in Baltimore.

Big Security Breaches

A financial analyst at Countrywide, the disgraced subprime mortgage company, was caught by the FBI selling two million consumer profiles – many with Social Security numbers included. He sold a batch of 20,000 records in exchange for \$500 every week. Another 4.2 million people were exposed to identity theft when credit and debit card numbers were stolen as they were being authorized in Hannaford grocery stores in Maine and Florida. To date at least 1,800 people actually suffered fraud because of the breach.

The list goes on: Two million people exposed by a breach at the University of Miami; almost three and a half million placed at risk by Colorado’s Division of Motor Vehicles, which regularly transmits huge packages of personal information over the Internet with no encryption.

This is the rule, not the exception. Data was protected by a password in only 8.5 percent of all reported breaches in 2008, according to ITRC, and only 2.4 percent of the breached information was secured through encryption or other protection.

“It’s bad enough that attackers are able to get inside the perimeters of the companies, but they certainly shouldn’t be able to find any unencrypted customer records once they get there,” Dennis Fisher, executive editor of *Computer Weekly*, wrote in his column in 2008. “The same goes for government agencies. Just do it.”

Steal My Skyscraper, Please

The *New York Daily News* scored a journalistic and real estate coup in December when it “stole” the Empire State Building, valued at \$2 billion, in just 90 minutes. The newspaper managed this feat simply by filing a fake deed with the New York City Register’s Office,

claiming that the famous building had been bought. The application stated that Fay Wray, star of the original King Kong movie, had witnessed the purchase, and that famed (and dead) bank robber Willie Sutton had served as the notary public.

The newspaper’s funny stunt had a serious purpose, showing just how easy it is for identity thieves to steal the deed to properties in New York City (and raises the question of how easily this could be done elsewhere). All you need is a notary stamp, which costs \$30.

“Once you have the deed, it’s easy to obtain a mortgage,” Richard Farrell Brooklyn Assistant District Attorney, told the *Daily News*. “Crooks go where the money is. That’s why Willie Sutton robbed banks, and this is the new bank robbery.”

The newspaper generously returned the skyscraper to its rightful owners.

Big Bust in Biggest Identity Theft Case Ever

The biggest identity theft ring detected to date was also one of the boldest. According to an indictment filed by the U.S. Department of Justice, 11 members of a crime ring drove around the country with laptops that scanned for unsecured wireless networks. They eventually worked their way into systems run by Barnes & Noble, OfficeMax, BJ’s Wholesale Club Sports Authority, DSW Shoes and Dave & Buster’s, installing “sniffer” programs to steal credit card numbers, account information and passwords.

The team’s biggest coup was its hack of TJX Companies, Inc., owners of the TJ Maxx and Marshalls chains. Burrowing into TJX’s unsecured wireless network, the crime ring stole at least 45 million records (some experts suspect the total actually reached 94 million). Some of the account information was printed onto blank debit cards, which were used to withdraw tens of thousands of dollars from ATM machines.

The alleged thieves were indicted this past August. “So far as we know, this is the single largest and most complex identity theft case ever charged in this country,” US Attorney General Michael Mukasey told *The Boston Globe*.

TRENDS TO WATCH IN 2009



IDENTITY THEFT SWELLING IN A SINKING ECONOMY

The dim and darkening economic outlook means more Americans face foreclosure, bankruptcy and collections. Unfortunately, where there is crisis, there is opportunity—in this case, for identity thieves looking to capitalize on people’s desperation.

Consumers with poor credit may look to deals offering credit cards, debt consolidation and foreclosure avoidance regardless of credit history. Other lures may include offers of undemanding, great-paying jobs, or easy money to be made from foreclosed real estate. Many people holding out such too-good-to-be-true opportunities will be scammers looking to steal identity information.

“People are growing increasingly desperate, which is why these scams work,” says Richard Hagar, a mortgage fraud expert who trains law enforcement agencies in how to spot investment crimes.

And many of the people who do file for bankruptcy protection may expose their identities to theft, because they are required to give private information including Social Security numbers on court forms that are open to the general public. As banks reduce the amount of credit available to consumers, we likely will see an uptick in old-fashioned fraud using stolen or counterfeit checks.

THE INSIDER THREAT INTENSIFIES

Last year we saw a disturbing rise in the number of security breaches caused by current and former employees stealing data. With businesses laying people off and the underground identity theft economy becoming better established, look for this trend to worsen in 2009. After all, people who’ve been laid off may have a greater economic incentive to make money, and they’re not likely to feel any loyalty to former employers. Workers at banks, insurance companies and health care institutions have access to an unprecedented amount of private data that is growing in value as identity thieves hunt for consumers with solid credit ratings. Each of these organizations faces severe economic pressure, which could translate to an increased push from opportunistic insiders. Perhaps increased employee screening will result.

NEW WORDS, NEW TECHNOLOGY FOR OLD SCAMS

Some of us language traditionalists gave a heavy sigh of defeat when we realized that the ugly word “vlogging” (for video blogging) had become part of the media lexicon. As if that weren’t bad enough, we now have “twishing”—a takeoff on phishing (itself a linguistic abomination)

that uses messages on Twitter, the social networking service, to steal passwords and other personal information. Just as in a phishing attack, identity thieves go twishing by sending Twitter messages that link people to fake websites that resemble real ones, and that ask them to enter their usernames and passwords. Those texting keystrokes are recorded, saved in the thief’s database, and sold on the black market.

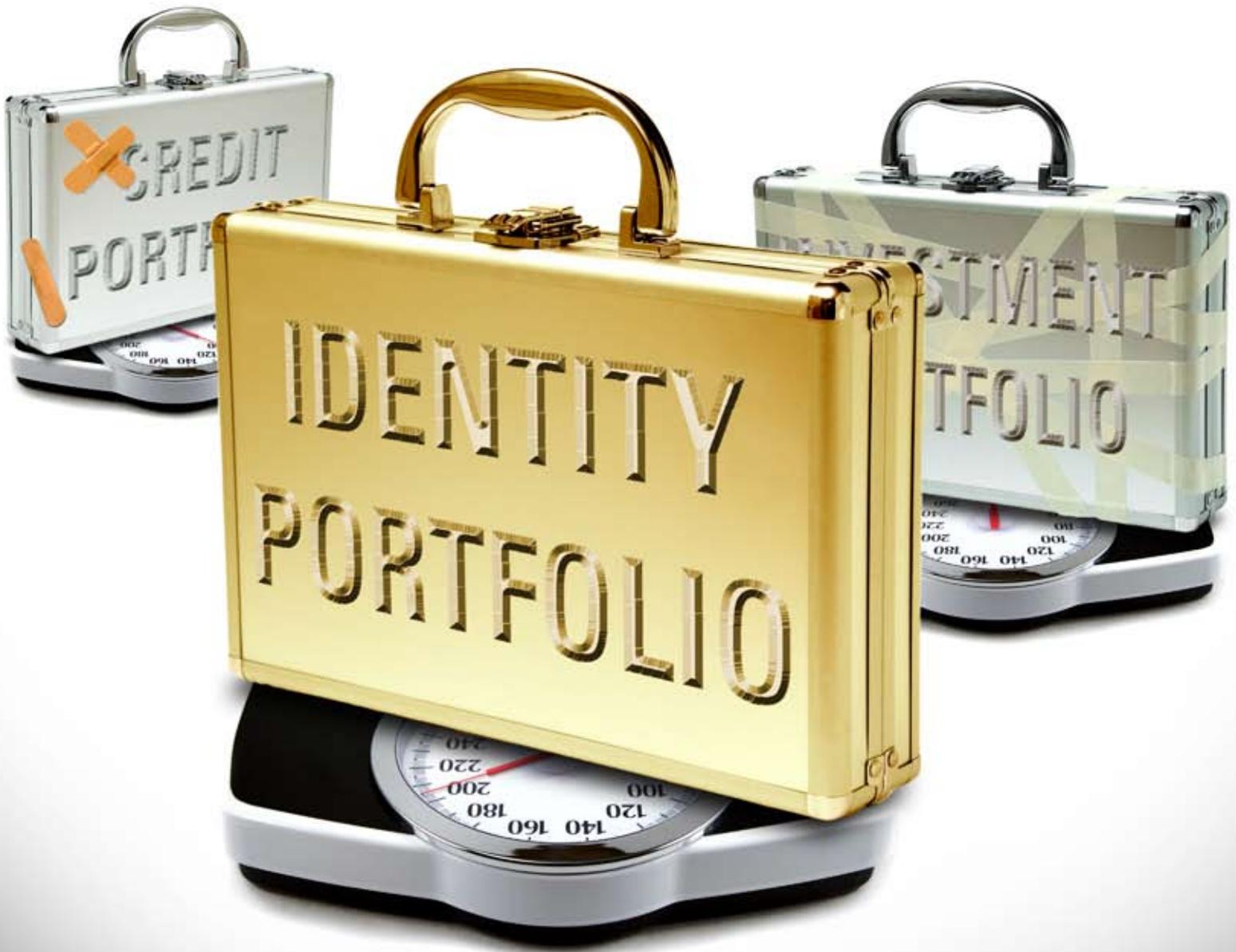
THIEVES WON’T GET DUMBER

In 2008 the number and sophistication of identity-stealing malware packages took a big jump. Because much of this activity is run by organized crime syndicates in Eastern European countries that lack both tough anti-fraud laws and sophisticated law enforcement capable of tracking and cracking down on these types of crimes, most experts agree that Internet-based identity theft stands to get worse in 2009.

“The overall trend is that we will see more attacks, and they will be programmed to do more nasty things,” says Zulfikar Ramzan, senior advanced threat researcher at Symantec.

Worse yet, the increased threat comes at a time when most organizations are looking to trim fat off their budgets. We’re hoping that doesn’t cut into the lean, the critical security work of respective IT departments.

MANAGING YOUR...



Everybody knows what an investment portfolio is, especially those of us who've seen portfolios take a nose-dive along with the rest of the economy. But what about an identity portfolio? Confused? Like finances, our identities must be managed and protected. That's why it's time to start treating the various components of your identity as part of their own respective portfolio. After all, a carefully managed and tended identity could be just as critical to your long-term happiness and financial well-being.

In an era when so many people are angling to steal identities for profit, honest citizens must adopt a new paradigm that values privacy and is wary of all requests for personal information. When it comes to getting the things we need in life—a mortgage, a car loan, or reliable health care—our overall identity is more valuable than a single credit score or Social Security number.

Right now our personal information is coursing through the electronic systems of insurance companies, government agencies, credit card

conglomerates, and all the major and minor institutions with which we come into contact every day.

While there is no magical way to prevent identity theft wholesale, there are steps you can take to mitigate potential threats. The following strategies will help protect your identity portfolio in the long run, no matter which direction your investment portfolio is headed now.

MEDICAL RECORDS

Middlemen in the health care industry are spreading identity information from your doctor's office to medical databases in India. But there are steps you can take to make sure that your medical records are not being misused.

- Keep copies of your own medical files. Carefully review all statements sent to you by snail mail or email to look for potential problems.
- Contact your medical insurance provider regularly—at least once a year—to review all benefits to make sure that no one else is receiving health care in your name.
- If you find any false or fraudulent items in your medical records, dispute them immediately by contacting all the relevant parties (your doctor, hospital, insurance company, etc.). If it appears that identity theft was involved, file a police report.

FINANCIAL DATA

Your Social Security number is the most important piece of your identity portfolio, followed closely by your credit and bank account numbers and passwords. There are a number of things you can do to keep them safe.

- Guard your Social Security number by regularly checking the Social Security Administration's website, where you can make sure that no one else is working, paying taxes, buying homes or making any other fraudulent purchases using your Social Security number. Go to: <http://www.ssa.gov/onlineservices> and click on "Check your information and benefits. After creating an online account, you can check your records for fraud. Also, carefully read your annual tax statement from the Administration.
- Check your bank and credit card statements at least once a month – perhaps daily if you use an online account—to make sure that no one has gained access to your accounts.
- Keep your bank and credit statements, but shred anything else that might contain account numbers or any other personal information.
- Get a free annual credit report. The three major credit reporting agencies—Equifax, Experian, and TransUnion – are required to provide you with a free copy of your credit report once every 12 months using the authorized website: <http://www.annualcreditreport.com>.

- Never give personal information over the phone unless you have initiated the call, or you know the caller well.
- Photocopy all your sensitive documents and store them in a secure location.
- Never carry your Social Security card or too many credit cards in your wallet.

PUBLIC RECORDS

Government agencies maintain vast databases of private information, many of which are free and open to the public, often online. There isn't much you can do to avoid handing your records over to the government. But you can:

- Search the websites of government institutions. Search the databases of your local courts to make sure that no one has committed a crime or obtained a lien in your name. If you buy and sell houses, check your county assessor's office to make sure there are no errors in their records. If you find your personal information in their online databases, contact the clerk's office in those agencies and find out if there's any way to remove your information from the public files. Many agencies have policies for this, but only do so when requested.
- Pay a private company to run regular searches of government databases for your personal information. (But beware of any company that guarantees identity theft protection. There are so many ways to steal someone's identity that it's impossible to fulfill such a promise.) In most cases, the company will alert you by email if your information has been made public. This allows you to follow up with the agency to remove the data, or at least correct any errors.

HIGH-TECH SOLUTIONS

Computer experts tell us again and again that when it comes to identity theft, we are our own worst enemies. Technology is advancing rapidly, and most people simply haven't kept up with all the different ways they need to protect themselves from scams. Here are the major ones.

- Buy software to protect your computer from attack. Trojans are the worst of malware; they secretly load onto your computer and steal your logins, passwords, credit card numbers and Social Security numbers. Even the most basic, over-the-counter programs such as Norton Anti-Virus can stop these programs and protect your identity.

- Save all your usernames and passwords in a lockbox on your computer.
- Most people use the same password for every website. That's obviously dangerous, but who can remember a different password for each account? The best way is to create different logins for every account you have, and save it all in a walled-off corner of your computer that's encrypted and password-protected.
- Turn your entire computer into a lockbox. If you're really worried about someone stealing information from your computer, you can seal it off by encrypting all of your files, with a secret password that turns off the encryption.
- Be smart online. Do not go sprinkling your name and credit card number around the Web like so many Spring raindrops. To minimize the exposure of your data, set up online bill pay through your bank account to deal with regular payments. For one-off purchases, consider obtaining a unique credit card number that can only be used once and cannot be traced to your credit card (Citibank and PayPal are among those that offer this service). Don't use an email address or username consisting of your actual name – use abbreviations or numbers instead. Don't tell people in chat rooms where you live. Remember that everything you type, especially online, will live in a database forever, so be careful about what private information you expose to the public.

KNOW WHO'S HANDLING YOUR DATA, AND WHETHER THEY'RE DOING SO RESPONSIBLY

Granted, this one's tricky, since so much of our data is handled by third-party contractors, and it would be nearly impossible to track which contractor is doing what with our data. But whenever possible, don't be afraid to ask questions and ensure that any company that you know is handling your data values strict data security and has the latest protocols in place—and that they also hold their third-party contractors to high security standards. If you're aware that an organization is using a contractor with a reputation for bad data handling, or have other evidence that data security is not high on their list of priorities, make your voice heard—let them know that your data is highly proprietary information and you require data handlers to treat it as such. If you can take your business (and your data) elsewhere, do so. And contact your state Attorney General while you're at it.

The concept of “identity” can be a difficult one to grasp. Set aside the concept in the grand philosophical “Who am I?” sense for now – though that, too, is an elusive animal, and it can’t be separated from other facets of “identity.” For now, I’m talking about the identity that exists in the tangible world, largely on paper. Though many of us know all too well that when something goes horribly wrong with our on-paper identity, it can shake us to our foundation and raise some rather existential issues.

An identity comprises many disparate pieces of data – our name, our personality, our hair and clothing styles, our Social Security number, etc. – and unites them into a whole that is greater than the sum of the parts. It’s highly regrettable if someone steals one of your blank checks, but many of the other parts that add up to your identity are still intact, so you’re still you. Or so you would assume, until you see just how much damage one stolen check, or one leak of your identity data can do.

Let’s say a thief uses that stolen check to help finance the purchase of, say, 1,000 acres of prime Russian farmland. Suddenly you’re not the “you” you used to be, because now

you’re broke. All that you’ve worked for, all that you’ve saved, has been taken from you. Even if the bank returns the stolen funds to your account, the time spent lobbying and waiting for the return of your funds can have a devastating impact on your life. Or if someone gets arrested for burglary or any other crime, and gives the authorities a bogus identification card with your

data on it? In the eyes of the FBI or the police, “you” are now a suspected criminal.

A living entity

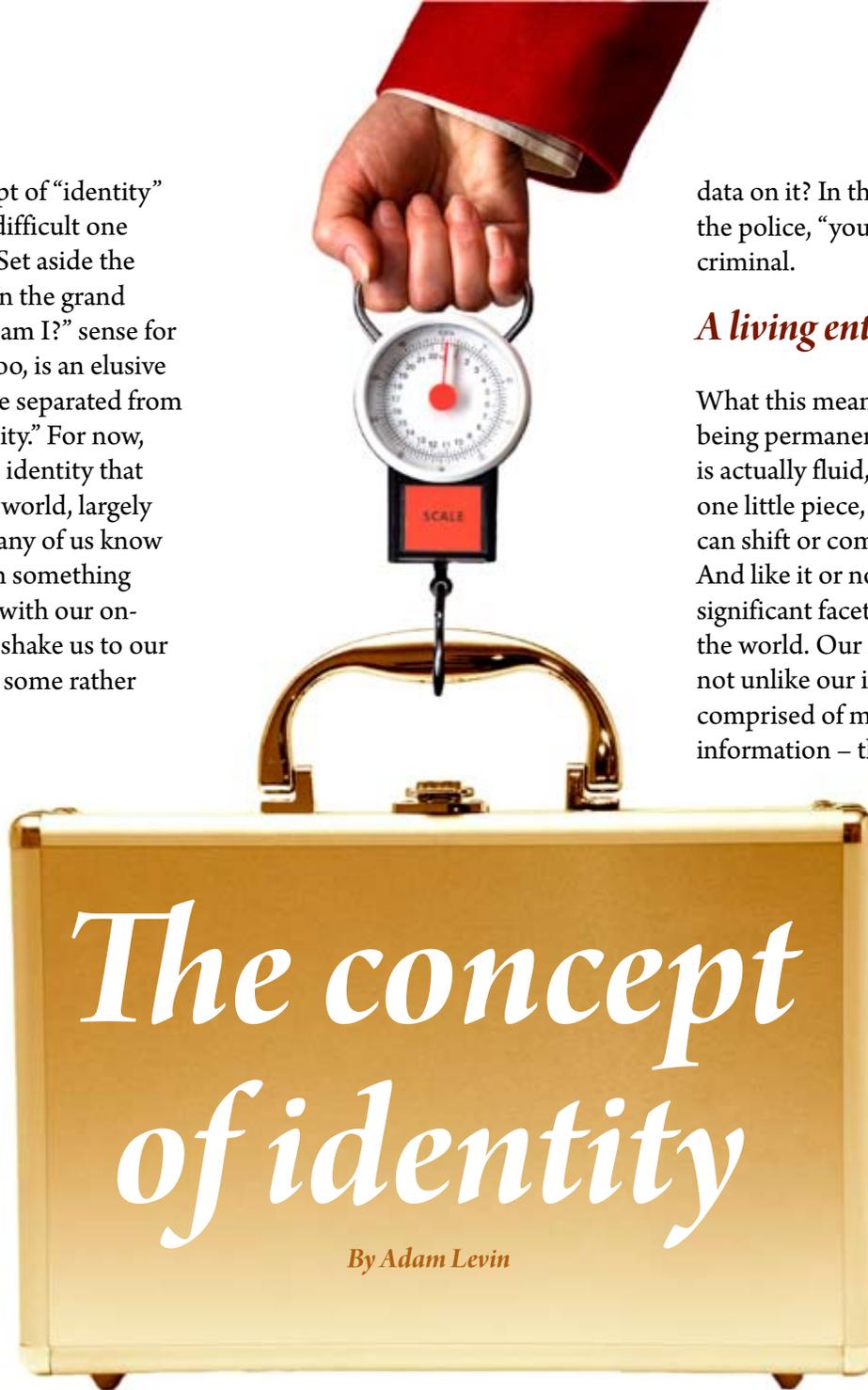
What this means is that, instead of being permanent and solid, “identity” is actually fluid, variable. Change one little piece, and the entire facade can shift or come crashing down. And like it or not, our finances are a significant facet of our identities in the world. Our financial portfolios, not unlike our identities, are comprised of many smaller pieces of information – the number of stocks

I own in Company X, or the rising value of my home after my neighbor sells his for a profit.

And just as most of us have confidence in the strength of our identities, the majority of Americans had confidence in their financial portfolios, at least until very recently. We’ve experienced a series of booms in

the last ten years – the tech boom, the Wall Street boom, the housing boom – in which many peoples’ identities seemed to drastically change. They became rich. Even people who didn’t directly benefit watched as their retirement investments grew over time.

We know now that much of that growth was hollow, that the Wall



Street “boom” was really just an overleveraged bet on American home buyers, who were themselves overleveraged to the hilt. Some, including people who trusted Ponzi schemer Bernie Madoff, were wiped out entirely. Everyone else has been affected by falling home values and declining retirement accounts.

The same is true with identity theft. Some victims suffer minimal damage. A stolen credit card might lead to a few hours on the phone with Visa complaining about fraudulent charges, and our credit issue is resolved with relative ease. If he or she is lucky, the victim won't experience any further criminal activity.

However, many others are less fortunate. We've seen cases where an identity thief hijacks everything – Social Security number, address, credit cards, checks, bank and cell phone accounts – completely destroying the victim's financial life for years to come.

Gaining control

Our identities and investments are both entities that must be managed. Looked after. Protected. An identity portfolio is composed of many pieces of data – from medical records, Social Security profile, credit files, financial data, public documents – and it requires constant care because it's expanding all the time. So are the threats. It's no longer simply a matter of shredding our private documents. Thousands of people post their private identity information on Facebook and Twitter every day. Medical records companies are contracting with database

subcontractors in developing countries. Workers in the banking and insurance industries enjoy more access to our identity data than ever before. As their industries contract during the financial crisis, those workers will have more incentive to steal our information for profit.

That's why it's helpful to think of the identity as a portfolio: Lists of assets and liabilities that can be aggregated and tracked. No one would look only at the value of his 401(k) to determine his wealth – what about his house, stocks and bonds? Only when they're all added together can we see how we're really doing.

In a similar way, one cannot – and should not – look inside one's wallet, confirm that all credit cards are in their respective sleeves, and assume that means that one is safe from identity theft. For one, your credit card number could exist in a database that's accessible to thieves. And don't forget that there are still government databases and dumpster divers to worry about.

By the same turn, you wouldn't walk into a grocery store and tack your credit card number to the community bulletin board. That would expose you, rather obviously, to credit fraud risk. But every day, millions of Americans log onto the Internet with no antivirus software protecting their computers. These are the same computers they use to pay their bills, manage finances, and write personal and professional letters containing private information. One of the most important ways to invest in a solid identity portfolio is to buy and install programs that protect your computer. After all, you wouldn't be managing it

very well if you were leaving it more accessible to thieves.

This is why we must expand our concept of “identity” to include all these new permutations. Only by recognizing the whole of our identity portfolios, and understanding that they belong to us, can we begin to take better control of our identities

Deeper issues

Now that we've made ourselves clear on the identity portfolio concept, there lies a sleeping giant that threatens to wake and potentially undermine any well-intentioned effort at managing your identity.

It is: Denial.

This mythical beast has always existed, but is all the more prominent – and dangerous – in a bad economy. Just like we may want to avoid watching what we believe is the hopeless and inevitable downward spiral of our investment portfolios, we may not want to face what we might find in our identity portfolios – whether the items of misery have been wrought by circumstance, by our own hands, or by the hands of others. As tempted as we may be to forgo looking at dwindling bank accounts and inflating credit card statements, anything to block out more potential bad news, this is the worst possible time to sacrifice your identity on the altar of avoidance. In a time when thieves are redoubling their efforts to siphon all they can from consumers, they're counting on their friend Denial to keep consumers from being vigilant.

Don't hand over the battle so easily. ■