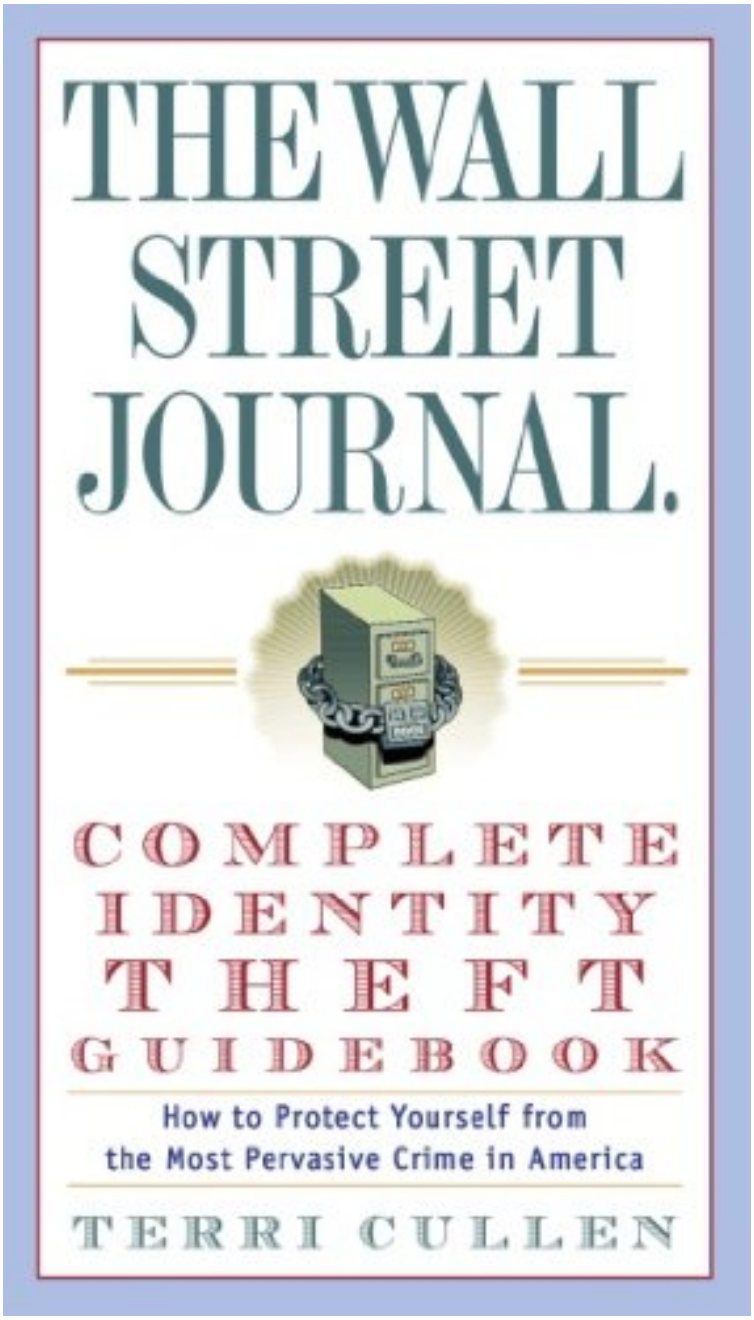
The Wall Street Journal. Complete Identity Theft Guidebook: How to Protect Yourself from the Most Pervasive Crime in America (Wall Street Journal Identity Theft Guidebook: How to Protect)

Terri Cullen



#1087352 in eBooks 2007-07-10 2007-07-10File Name: B000UDNBPS | File size: 75.Mb

Terri Cullen : The Wall Street Journal. Complete Identity Theft Guidebook: How to Protect Yourself from the Most Pervasive Crime in America (Wall Street Journal Identity Theft Guidebook: How to Protect) before purchasing it in order to gage whether or not it would be worth my time, and all praised The Wall Street Journal. Complete Identity Theft Guidebook: How to Protect Yourself from the Most Pervasive Crime in America (Wall Street Journal Identity Theft Guidebook: How to Protect):

41 of 43 people found the following review helpful. THE Best Identity Theft Book AvailableBy O. Merce Brown*****I have read several identity theft books, and this book from the Wall Street Journal is by far the best. For starters, it is short, containing JUST the information you need to know. The first half of the book is about how to prevent identity theft. The second half of the book is about how to recover from identity theft. It is so helpful for me to have everything I need to know collected succinctly all in one place.The book covers things you can do to prevent identity theft and exactly how the latest scams are perpetrated so that you can be aware (including utility theft, employment identity theft, medical identity theft, and home equity theft). It covers understanding your credit report, including credit monitoring tools and other credit tools (including the differences between a credit alert and a credit freeze, something I had been confused about); the book identifies your credit report as the single most important document for protecting your identity. There are many examples of credit reports and how to interpret them. There is also information about identity theft and technology, made understandable for pretty much anyone.The second half of the book includes resources for identity theft recovery---numbers to call, sample letters, sample logs, laws, and more. Hopefully, by reading and implementing the first half of the book you will never need the second half of the book. Nothing is ever totally foolproof against identity theft, of course, but there are so many basic things you can do to minimize your risk of becoming a victim.Despite including all of this information, the book can be read by anyone in 4-5 hours. In my opinion, this is information everyone should be aware of. Law enforcement is overburdened and cannot be relied upon to protection; each person has to take personal responsibility to protect themselves, and this book is all you need to do so. You'll have work to do after reading the book, of course, but it will be worth it. Save you money, and if you want to just buy one book, make it this one.Highly recommended.*****0 of 0 people found the following review helpful. Four StarsBy M. MurphyItem received on time and very informational10 of 10 people found the following review helpful. Valuable resourceBy CustomerA thorough, easy-to-read depiction of how identities are stolen, how you can protect yourself, and what to do if your efforts fail. Significantly, the book points out that identity theft often is an inside job; i.e., it isn't a hacker in Russia, it is one of your nearest and dearest (?).

It could happen when you make a routine withdrawal from an ATM, respond to an e-mail asking for information about an online account, or leave a new box of checks unattended in your mailbox. Identity theft is one of the easiest crimes to commit in Americamdash;and one of the hardest to prosecute. As thieves become increasingly clever, Americans have more reasons than ever to fear this elusive, ubiquitous crime. Now therersquo;s a book to help you beat it.In two easy-to-understand sections, Terri Cullen, The Wall Street Journalrsquo;s expert on identity theft, first walks you through the most common types of identity theft and how to arm yourself against them, and then leads victims step-by-step through the process of reclaiming a stolen identity. The average victim loses more than $6,000 and spends approximately 600 hours negotiating the complex bureaucracies and paperworkmdash;this book will help save time and effort by laying out the process. And by following the advice in the first half, you may never need the second!Yoursquo;ll learn:bull; how to avoid the most common scams, from ldquo;phishingrdquo; to ldquo;dumpster divingrdquo;bull; why children under eighteen are the fastest-growing target, and how you can protect your familybull; why your credit report is the single most important document for protecting your identitybull; how to use the sample letters, forms, and other useful tools inside for recovering from identity theftIn todayrsquo;s marketplace, your two most valuable assets are your credit and your identity. No one should be without this vital guide to protecting them.From the Trade Paperback edition.

From BooklistIdentity theft is one of the fastest-growing crime segments worldwide, yet the laws in place to prosecute these offenses are scant and rarely enforced. Cullen, assistant managing editor and personal finance columnist for the Wall Street Journal Online, explains that there are really two broad variations of identity-related crime: identity theft, which is impersonation of someone else to get a job or hide one's own criminal record; and identity fraud, the use of another person's credentials for monetary theft. Getting someone else's personal information is surprisingly easy, but Cullen shows in part 1 how, through simple diligence such as shredding documents and protecting yourself online, you can avoid having to follow the directions in part 2, where she explains how to clear your name should you become a victim. The average identity-theft victim will have to spend 600 hours clearing his or her good name. This is a straightforward guide broken up with interesting sidebars and plenty of charts, in the Wall Street Journal tradition. Siegfried, DavidAbout the AuthorTERRI CULLEN is an assistant managing editor and award-winning personal-?nance columnist for The Wall Street Journal Online. She lives in New Jersey with her husband and son.Excerpt.

CHAPTER 1What Is Identity Theft, Anyway?Jerome Powell remembers being irritated with himself for not paying closer attention to his driving. When the Mountain View, Colorado, police carrsquo;s blue lights came on behind him, Powell, a government contractor, had just driven through a yellow light as it turned red. Now he would be late for his next appointment. He apologized to the officer and handed over his driverrsquo;s license and insurance information. He watched in his rearview mirror as the officer radioed from his cruiser for a license check.It seemed to be taking a long time to write a routine ticket. Finally, the officer approached Powellrsquo;s window and told him to get out of the car. Powell was stunned to find himself under arrest on two outstanding felony warrants. He was shocked and humiliated as the officer made him put his hands behind his back and then cuffed him and read him his Miranda rights. The Navy veteran spent hours in jail, shaking from fear that he might wind up charged with a crime he didnrsquo;t commit.The warrants for his arrest were issued in 2003, when a thief used Powellrsquo;s driverrsquo;s license to buy more than $10,000 in computer equipment and other items. Despite overwhelming evidence that it was a case of identity theftmdash;the stolen goods were delivered to the apartment of a career criminal who bore no resemblance at all to Powellmdash;he was forced to spend several thousand dollars to post bond and get a lawyer to clear his name.Jerome Powellrsquo;s unnerving and expensive experience is a true case of identity theftmdash;the thief used Powellrsquo;s driverrsquo;s license to impersonate Powell. Not to be picky about it, but what the media and most people call ldquo;identity theftrdquo; is actually an umbrella term for two different crimes: identity theft and identity fraud. As in Powellrsquo;s case, identity theft occurs when criminals steal personal information and use it to impersonate the victim. An illegal immigrant using a stolen Social Security card to get a job is a good example of such an impersonation, as is a driver who has lost his or her license because of multiple convictions for driving while intoxicated and buys a fake driverrsquo;s license from an underground dealer containing the name and information of an identity-theft victim. True identity theft accounts for about a third of the 685,000 identity crime complaints reported to the Federal Trade Commission in 2005.Far more common is identity fraud. It happens when thieves obtain a victimrsquo;s sensitive personal information to steal money from bank accounts, buy goods and services with existing credit-card accounts or use the data to open new credit lines. The shocking thing is that these types of criminals are frequently people we know. Such betrayals by family or close friends are emotionally draining and almost certainly underreported since victims often find it difficult to report the crime or feel pressured by family members to keep the theft quiet.Not Abigail Kelly. Abigail had given her Social Security number to her sister Delia after Delia said she was going to make Abigail the beneficiary of her life-insurance policy. Delia promptly used Abigailrsquo;s information to open fraudulent credit and utility accounts. As a result, Abigail not only suffered damage to her credit history, but she didnrsquo;t get the job after an employee background check turned up an arrest warrant for an unpaid home heating bill in her name in Maine. Abigail had never even been to Maine. But Delia lived there. Abigail later learned that her sister was behind numerous accounts opened in her name, though Delia wasnrsquo;t arrested or charged with any crime. Local law enforcement refused to get involved in what looked like a family dispute, so Abigail wound up suing her sister in civil court instead. After Abigail sued her, Delia finally agreed to pay most of the $50,000, but the incident tore their relationship apart. ldquo;You are dead to me,rdquo; Delia later told Abigail.Routine one-on-one crimes are the most common and are largely ignored by the media and, unfortunately, many times by law enforcement. Itrsquo;s the big-time scams and plots that get the attention. In August 2005, employees at Sunbelt Software Inc. stumbled upon a massive identity- theft ring while researching ldquo;CoolWebSearch,rdquo; a dangerous software program that hijacks Internet servers and Web home pagesmdash;as well as other browser applications. The software was routinely obtaining and broadcasting data such as individual names, bank-account numbers, passwords and PINs, and other extremely sensitive personal information from millions of infected computers. That investigation continues today.Itrsquo;s surprisingly easy to become an identity thief or fraudster by joining the ranks of criminals who simply buy the information from any number of legal or illegal sellers of sensitive consumer data. Once little-known to most Americans, the data-broking industry burst into the spotlight in February 2005, when ChoicePoint, a seller of consumer data to financial institutions and government agencies, disclosed that criminals posing as legitimate businesspeople had purchased personal information on 145,000 people. (Later, the figure was revised to 162,000.) Americans were staggered by the types of personal information being sold by ChoicePoint, including their names, their spousesrsquo; names, current and previous addresses, phone numbers, Social Security numbers, names of employers and even information about family members and neighbors. While individuals can sometimes buy such data legally, most legitimate data brokers sell only to corporate customers. But the fact that therersquo;s no regulation of legal data sales means itrsquo;s easier for criminals to get their hands on your information.COMPANIES RESPOND TO DATA BREACHESHerersquo;s a sampling of what some specific companies and organizations have offered to do in response to disclosures that sensitive consumer information was lost or stolen from their databases.Time WarnerA contractor moving backup tapes discovered that one tape containing data, including many Social Security numbers, on 600,000 current and former employees, was missing. Time Warner offered a year of free credit-monitoring service.Fidelity InvestmentsA Fidelity employeersquo;s laptop, containing personal information on 196,000 current and former Hewlett-Packard workers, was stolen from a rental car. In response, the fund giant alerted credit-reporting agencies and offered free credit-monitoring service for a year to

current and former HP employees.Tufts UniversityAdministrators discovered unusual activity on a university-owned computer with data, including some Social Security numbers, on 106,000 alumni. Tufts set up an 800 number for assistance and encouraged people to put alerts on their credit reports, but did not offer to pay for monitoring.University of California, BerkeleyA laptop was stolen containing Social Security numbers belonging to 98,000 students, alumni and applicants. UC Berkeley set up a hotline and encouraged people to put alerts on their credit reports, but didnrsquo;t offer to pay for monitoring.Wells FargoFour computers containing sensitive personal data for thousands of people were stolen from a vendor that prints loan statements. Wells Fargo responded by offering a year of free credit monitoring using its own service.Source: The Wall Street Journal Online.QOver the last five years, media coverage has increased as dozens of companies, universities, government agencies and other organizations have reported that vast amounts of sensitive consumer information was either lost or stolen. The list of companies that have reported lost or stolen consumer information reads like a ldquo;Whorsquo;s Whordquo; of big business: Bank of America, Fidelity, Hewlett-Packard, Time Warner and Verizon, among others. In some instances, data-storage tapes went missing or laptops containing sensitive information were stolen; in others, employees of the companies or organizations obtained unauthorized access to the information. Even the federal government isnrsquo;t immune. In 2006, thieves stole data on about 26.5 million military personnel from the U.S. Department of Veterans Affairs. The laptop with the missing data was recovered a month after it was stolen, and two teens were arrested for the theft. But the department stumbled twice more, first when it canceled the credit-monitoring service it had offered the victims of the laptop theft, infuriating innumerable veterans who were counting on it to help protect the breach of their sensitive information. And then it happened again! Another department laptop disappeared. Needless to say, there are some decidedly unhappy vets wondering just how inept the department can get.Not surprisingly, victims are beginning to fight back in the courts against companies and organizations that report breaches of sensitive consumer data. In June 2006, a coalition of veterans groups filed a class-action suit against the federal government in the U.S. District Court in Washington, D.C., seeking $1,000 in damages for each of the roughly 26.5 million military personnel, both current and former, whose data was on the stolen laptop mentioned earlier. In July 2005, a group of plaintiffs filed a class-action lawsuit in California Superior against CardSystems Solutions Inc. after the company disclosed that computer hackers had obtained data on about 200,000 credit- and debit-card accounts.GARDEN VARIETY IDENTITY FRAUDIrsquo;ll get into some of the more exotic types of identity theft and fraud later. For the moment, letrsquo;s take a look at some of the most common forms of identity crimes. It isnrsquo;t hard to guess that by far the favored tool of identity thieves is the ubiquitous credit card. We all have them and we love to use them. So do identity thieves. The Federal Trade Commission (FTC) found that 26 percent of all complaints of identity fraud in 2005 involved fraudulent charges on an existing account or new accounts opened using lost or stolen consumer information.How easy is it to fall victim to credit-card fraud? Let me count the ways.We use credit cards so often and in so many placesmdash;online and in personmdash;that it is almost impossible to avoid tripping up and revealing your account information to a potential thief. I shudder to think of how careless I was with my credit-card account information before I discovered that Irsquo;d become the victim of identity fraud. I would routinely crumple up credit-card receipts containing my signature and entire account number and then casually toss them in the nearest trash receptacle for a would-be thief to snatch. When making travel reservations at work, Irsquo;d broadcast my credit-card number when giving it out to hotels or car-rental agencies, so that anyone within the sound of my voice could jot it down. When using ATMs, I worried more about the guy behind me invading my personal space than I did about whether the offending person was ldquo;shoulder surfingrdquo; to learn my accountrsquo;s password. Online, I rememberedmdash; occasionallymdash;to check to see if a sitersquo;s Web address started with the telltale ldquo;https://rdquo; and the tiny closed-padlock symbol at the bottom of the Web browser that indicated I was shopping at a secure site. I almost never checked sites such as the Better Business Bureau (www.bbbonline.org) and TRUSTe (www.truste.com) to ensure that the Web site I was using was a legitimate business.Then a phone call from my credit-card issuer made me aware of just how easy it is to fall victim to identity fraud. The companyrsquo;s representative said the company noticed Irsquo;d made two purchases within hours of each other using my cardmdash;one in New York, the other in France. Fortunately for me, the card company put the purchases on hold until it could contact me and verify that I had made them. I was shockedmdash;and a little scared. If my credit-card information had been stolen, what other personal information could the thief have?So now I pay close attention to things like keeping my voice down when making travel reservations or making sure no one gets too close in the ATM line. I also routinely monitor my credit-card statements online for signs of fraudulent charges. When shopping online, I always use a credit card, rather than my debit card, which is attached to my checking account, because federal law limits liability for unauthorized credit-card use to $50 per card, though many companies will waive this amount if they are notified of the charge in a timely manner. Some debit cards donrsquo;t have this kind of zero- liability protection against fraud, but, more importantly, even if your bank offers zero-liability coverage on your checking account, it could take weeks to recover your account after a thief has wiped it outmdash;and you could find yourself vulnerable to bounced-check fees on outstanding payments.CALLING ALL THIEVESAfter credit-card fraud, phone, cable and utilities fraud is the second most common form of identity theft, making up 18 percent of all complaints reported. Dishonest people steal personal

information in order to apply for cell-phone contracts or improperly gain access to cable, telephone, gas and electric energy, or other types of utilities. Itrsquo;s a difficult crime to combat, which is why itrsquo;s so popular among identity thieves. They open accounts in one place and then quickly move on to the next to avoid capture. By the time victims discover the crimes, the thief is usually long gone.Kevin Scott of Philadelphia discovered he was the victim of utility fraud when he requested a copy of his credit report after being denied a loan. A thief had obtained Scottrsquo;s Social Security number and used it to open utility accounts at several addresses, racking up thousands of dollars in phone, cable, gas and electric bills. The utility companies allowed the criminal to open these accounts despite the fact that duplicate accounts already existed in Scottrsquo;s name at his true address. They also never bothered to contact him. He spent hundreds of hours clearing his good name at companies such as Bell Atlantic, Comcast Cablevision, PECO Energy and Philadelphia Gas Works. He was also frustrated because state and local law enforcers refused to help him track down the thief, despite the fact that authorities had his picture on file after the thief obtained a Pennsylvania driverrsquo;s license using Scottrsquo;s name.TAKE IT TO THE BANKBank fraud is only slightly less common than utilities fraud, which is surprising given that banks are among the moresecurity-conscious businessesmdash;and fooling around with a bank can earn a thief a visit from the Federal Bureau of Investigation. Bank fraud accounts for 17 percent of reported identity-theft cases, with nearly 2 million Americans reporting that thieves transferred funds out of their checking accounts in 2004. The average loss per incident was $1,200. Fortunately, consumers rarely are left holding the bag. If the fraud is reported promptly, most banks wonrsquo;t hold the customer liable for losses resulting from the crime. While fraudulent loans accounted for some bank fraud, the most frequent types of fraud involved electronic funds transfers and forged checks.Mailboxes are the venue of choice for bank fraudsters. It isnrsquo;t difficult to recognize a box of checks sitting in a mailbox, although it takes a diligent thief to check dozens of mailboxes on any given day to find the occasional box of checks. More sophisticated thieves look for bill-payment envelopes left in the mailbox for pickupmdash;then use special chemicals to erase the ink and insert different names.