Preventing Identity Theft in Your Business

How to Protect Your Business, Customers, and Employees

Judith M. Collins

WILEY
John Wiley & Sons, Inc.

Preventing Identity Theft in Your Business

How to Protect Your Business, Customers, and Employees

Judith M. Collins

WILEY
John Wiley & Sons, Inc.

This book is printed on acid-free paper. ∞

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

Published simultaneously in Canada

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Collins, Judith M.
Preventing identity theft in your business : how to protect your business, customers, and employees / Judith M. Collins.
p. cm.
Includes index.
ISBN 0-471-69469-X (cloth)
1. Identity theft—United States—Prevention. I. Title.
HV6679.C653 2005
658.4’72—dc22

2004022093

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To victims of identity theft and employees who help prevent it

ACKNOWLEDGMENTS

More than a faithful colleague and meticulous research assistant, Sandra Hoffman is a valued friend. As associate director, Sandra diligently, skillfully, and solely managed the bustling activities of Identity Theft Crime and Research Lab for three months so that I could write this book. I publicly acknowledge that without Sandra this book would not have been possible. With deep appreciation, I thank you, Sandra.

I also am indebted to my editor at John Wiley & Sons, Tim Burgard. Tim took the time to read my manuscript and recognized its potential importance for businesses. He provided the logistical and organizational support necessary to bring this book to fruition and along the way provided many constructive suggestions for improvements. Moreover, throughout the summer of 2004, Tim routinely and consistently prompted me for the next "batch" (of chapters). Because of Tim, this book moved from "in progress" to "in production." Thank you, Tim, for the guidance you've given me and also for believing with me that this book can positively impact businesses and people.

With appreciation, I especially thank my son, Michael Collins. Michael read every word of every chapter and offered many recommendations for modifications. I made them all. I now find it difficult to adequately express my deep gratitude to Michael, who unselfishly shared with me considerable time and his intellectual talents in reviewing chapter writes and rewrites. Thank you, son, for your invaluable contributions.

And to Larry Collins, my husband, mentor, and enthusiastic supporter of each next "project," thank you for being alongside me throughout these life's adventures.

CONTENTS

PART II: IDENTITY THEFT PREVENTION

PART III: MONITORING IDENTITY THEFT

APPENDICES

PREFACE

All companies that engage in financial transactions are bound by law to establish and enforce information security programs to prevent identity theft. Security "standards" are required by at least five federal laws, including the Fair Credit Reporting Act, the Federal Trade Commission's Privacy Rule, the Banking Guidelines, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Safeguards Rule. But there are problems. Nowhere do any of these laws describe how to develop, maintain, and enforce an information security program. In effect, the laws fail to stipulate what constitutes an "information security program" or "standards" for security.

Granted, the laws do specify information technology (IT) security—the security of computers and networks. Indeed, the main theme at the September 2004 American Banking Association's Identity Theft Symposium was "Technology to the Rescue." Bankers were informed of online products and protections and advised to prevent identity theft by using tools such as encryption, authentication, and software programs that guard against email and other computer fraud. *But computers do not steal identities.*

Rather, recent studies indicate that at least 50 percent or more of identity thefts are committed inside the workplace by a dishonest few employees who steal the Social Security, credit card, banking, or other numbers from their coworkers and customers. Federal laws fail, however, to cover *people* within businesses who have access to personal identities and the work *processes* used to manage and maintain such information.

The federal laws fall short. Computer security alone will not work. To secure company borders from the threat of identity theft requires an inclusive and exhaustive three-fold approach to secure people, processes, *and* the IT property. And the techniques used to develop, maintain, and enforce such an information security program would use universally established and widely documented methods known to be reliable and valid and that are inexpensive and accessible for all businesses, large and small. Fortunately, such methods exist and so, therefore, do the security solutions.

Preventing Identity Theft in Your Business shows how employee-manager teams can develop a set of Security Standards using step-by-step instructions written in lay language and using methods from industrial and organizational psychology, the management sciences, and the field of criminal justice. The methods are inexpensive, comprehensive, and universally applicable to all businesses regardless of size, type, or geographic location. Within six months or less, employees and their managers can bring any company into compliance with all current as well as any future-enacted laws.

Preventing Identity Theft in Your Business shows how all companies can build effective corporate policies to protect the identities of employees and their customers without impacting budgets and business operations. What's more, these *Security* Standards incorporate *performance* standards: Businesses will meet regulatory requirements while gaining competitive advantages. Using strategies proven to be effective, personal and business identities no longer are jeopardized and financial institutions no longer risk noncompliance. In short, identity theft stops here.

INTRODUCTION

Identity theft can be prevented. Contrary to common thought, most identities are stolen from businesses; fewer are stolen from garbage Dumpsters or by online hackers. Although thefts do occur from these sources (as well as from homes, cars, and persons), the majority of identity thefts are committed inside the workplace by a relatively few dishonest employees who steal the personal identification data of their coworkers and customers—a company's most valued assets. To safeguard these potential victims, and the company's interests, the workplace must be secured.

Because identity thefts occur so often in the workplace, businesses also are victims. In his keynote speech at the 2000 White Collar Crime Summit in Los Angeles, California's attorney general, William Lockyer, warned that identity theft was the greatest threat to the financial economy of businesses and the entire United States. Since then, and despite his warning, identity theft has escalated worldwide and continues unabated. The reason in great part is that no international security standards exist to protect personal information, such as the identities of U.S. citizens.

Nevertheless, federal laws now require *all* businesses to secure personal identifiers and document this or risk being fined. Nowhere, however, are businesses told *how* they might do this. Granted, each of several federal laws recommends database and computer security—but computers do not steal identities. Information technology (IT) cannot by itself secure personal information because, and perhaps to some degree due to those already secured IT systems, employee insider theft is the source of most stolen identities.

In the field of criminal justice, when the source of a crime is known, the incidence of that crime can be mitigated and even prevented. *Preventing Identity Theft in Your Business: How to Protect Your Business, Customers, and Employees* shows how manager-employee teams (managers have the decision power to authorize employee-designed solutions) can use step-by-step instructions in a series of consecutively ordered exercises to combat identity theft in the workplace. *Preventing Identity Theft* is written with employees in mind, to help protect them and because employees are the key to securing the workplace.

Employees are the persons closest to the workplaces and work processes where identity thefts occur. Some employees perform the job tasks required to process, update, and otherwise maintain and manage personal information contained on applications, healthcare forms, payroll and benefits checks, and other documents, both paper and digital. Those employees are positioned to recognize the work processes most susceptible to identity thefts; and those employees, therefore, also are the key individuals capable of securing those work processes.

But what exactly is an "identity"? In the evolution of crime, identity theft is a particularly fast-moving, ever-changing, and overarching crime that facilitates many ancillary identity crimes. In Part I, therefore, the first priorities are to update yesterday's definitions of identity theft and report on recent events and trends that, disturbingly, point to even greater incidence and variations in identity crimes. Included in the text is a discussion on "identity rape," the insidious effects on victims (both persons and businesses), and several sections detailing facts on why identity theft may never be completely eradicated.

The material in Part I is based on knowledge derived from reported experiences in the Identity Theft Crime and Research Lab at the Michigan State University–Business Identity Theft Partnerships in Prevention, established in 1999. As director of the lab and through work with law enforcement and businesses, and as professor of Information Security Management at the MSU School of Criminal Justice, the author has come face-to-face with the crime, the victims, and even some of the criminals. The *insider* modus operandi of identity thieves is now well known—which is why this crime can be prevented. And, from 18 years of training and applied work as an industrial-organizational (I/O) psychologist, the author has developed applied management methods to do this.

Beginning in Part II and continuing in Part III, the chapters describe a Business Information Security Program using methods from criminal justice, I/O psychology, and the management sciences. Each chapter leads the manager-employee team through workshop exercises to secure personal identifying information across four fronts: personnel, processes, proprietary information, and virtual property—the e-business Web site.

The chapter exercises to secure personnel integrate security into the traditional functions of recruitment, personnel selection, organizational socialization, and performance feedback. All personnel functions, beginning with the very basic job analysis, must be driven by sensitivity to security. The teams learn where to obtain or how to develop valid and reliable security instruments that meet the Equal Employment Opportunity Commission guidelines and Title VII statutes for fairness in personnel practices.

For some people, personnel selection, appraisal, and other practices can be threatening. In *Preventing Identity Theft in Your Business*, employees and managers take the lead in preventing identity theft in the workplace. The team designs and then oversees the personnel functions that will safeguard their security at work to protect them from the dishonest few, often temporary or contract workers. Thus, exercises in several chapters are devoted to protecting a business's most important asset and the *first front*: the people.

In succeeding chapters, the team conducts information process risk assessments to prevent the theft of personal information as it is processed through sequential job tasks, thus securing the *second front*: the work processes. The focus is on the job *position* and not the incumbent employee, because people come and go but job positions remain relatively stable. And there is no need to personalize identity theft prevention. It is a *workplace* problem.

In the concluding chapters, the team (or teams) conducts a Web Site Risk Assessment of the virtual property—the *third front*—and the team then establishes a Customer Security Program. The Web Site Risk Assessment, unlike IT security audits or assessments, measures *customer perceptions* of e-shopping security while visiting the business's online store. The Customer Security Program provides feedback and outcome measures while also helping customers protect their *future* flow of personal information, thereby avoiding victimization. Throughout, the aim is to secure the *fourth front*: proprietary, personal information.

The chapter exercises, enhanced by the management solutions they produce, are grounded in scientific theory. Based on practices from criminal justice, industrial-organizational psychology, and the management sciences, and written in easy-to-understand lay language, the chapter exercises also rely on many of the same tools businesses already use to develop "quality" standards.

This quality-to-security adaptation will be an especially easy transition for many businesses whose employees are adept at formal brainstorming, flow-charting, and other effective quality management practices. The applications and instructions for the quality-to-security management exercises and for the (perhaps) less familiar I/O psychology exercises are accompanied with illustrations of specific examples.

Identity theft is a devastating crime that undermines the economy and the very security of these United States. Its severity is not to be minimized. Legislation continues to be enacted in keeping with the continuing evolution of the crime, but legislation alone will not prevent it. To comply, therefore, with current laws as well as those that will be enacted in the future, businesses need to adopt a practical approach with specific procedures that extend the quality practices already in place and simultaneously guarantee "information" security. Once completed, these objectives can comprehensively, consistently, and over time secure a business from the threat of identity thefts.

The final product is a Business Information Security Program (BISP) that can be established with minimal costs to serve as an international security standard. Financial institutions, healthcare organizations, and *your* business can now comply with federal laws, and prove it.

PART I

THE CURRENT STATE OF IDENTITY THEFT

> He that filches from me my good name robs me of that which enriches him and makes me poor indeed.
>
> Shakespeare, *Othello* (3.3180-86)

CHAPTER 1

WHAT IS AN "IDENTITY"?

The term "identity" is commonly used arbitrarily and imprecisely in popular media and literature, and the terms "identity theft" and "identity crime" are frequently used interchangeably. Occasional misuses or misinterpretations are not surprising because in the contemporary context, the traditional meanings underlying those concepts have become increasingly known as information and information technology (IT). Formal definitions of identity concepts are therefore in order.

IDENTITY THEFT VERSUS IDENTITY CRIME

The *Oxford English Dictionary* defines "identity" as "the set of behavioral or personal characteristics by which an individual is recognized." The traditional use of the word "identity" spoke to one's name, familial membership, and occupation (among other applications). The contemporary meaning of "identity" has, however, assumed a candidly IT connotation that extends traditional meanings to include such things as one's consumer and credit histories, financial accounts, and Social Security number. It is this contemporary usage of "identity" that is at issue when it comes to conceptualizing identity theft and identity crime.

Identity theft is a burgeoning crime of relatively recent origin. To be sure, identity theft is dynamic in nature, as it has evolved over time. As fast as new legislative definitions of identity theft have been framed and novel techniques for enforcing those definitions have emerged, identity predators have abandoned old methods in favor of new and sometimes ingeniously innovative approaches. As the crime has evolved, so also has its descriptions and definitions.

For instance, "identity theft," most commonly thought of as the theft of an individual's *personal* identifying information, has evolved to include a new twist: *business* identity theft.

Further, the theft and fraudulent use of Social Security numbers now assigned babies at birth has, most recently, led to *child* identity theft, much the same way the crime of adult pornography evolved to include those crimes on children. Also similarly, *child* identity theft is now considered a subset of a more general category of crime: *personal* identity theft. Additionally, "identity theft" is defined as a felonious crime per se, that is, as an offense in and of itself, wherein one party steals sensitive information from another, either an individual or a business entity.

Identity *theft*, however, is to be distinguished from identity *crimes*—those offenses committed using the stolen *personal* or *business* identifying information—or "identities." Thus, the conceptual relationship between identity theft and identity crime is that the former facilitates the latter. In short, stolen identities often are used to commit many other crimes, which is why identity theft also can be viewed as an all-encompassing or overarching megacrime. Legislation, investigations, and the prevention of identity theft can take different approaches, depending on the type of identity stolen. Thus, to mitigate and prevent identity thefts requires that each type of identity be clearly delineated: personal, business, and overarching.

"PERSONAL" IDENTITY THEFT

Personal identity theft is the unauthorized acquisition of another individual's personally sensitive identifying information; personal identity *crime* is the use of such information to obtain credit, goods, services, money, or property, or to commit a felony or a misdemeanor. "Personally sensitive identifying information" means a person's name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, demand deposit account number, savings or checking account number, credit card number, or mother's maiden name—information needed to obtain an original birth certification for a complete identity takeover. With a birth certificate, mother's maiden name, and a Social Security number, for example, other governmental documents and records can be accessed; a passport and visas successfully applied for; and driver's licenses, court records, and other information fraudulently obtained and used to commit identity crimes.

Perpetrators use stolen personal identities to drain checking, savings, and retirement accounts; create bogus checks; open new credit card and bank accounts; take over existing accounts; apply for telecommunication and utility services; obtain home, automobile, college-tuition and other loans; open retail accounts; purchase airline, rail, and other transportation accommodations; rent hotel/motel rooms; rent or purchase automobiles; pay for medical supplies, prescriptions, and healthcare services; obtain employment; engage in money laundering, drug trafficking, and other organized crime; and commit acts of terror against the United States. Some, but not all, of these crimes also are committed using stolen business identities, which are to be distinguished from personal identities.

"BUSINESS" IDENTITY THEFT

Business identity theft is the unauthorized acquisition of a business's "business identifying information." Business identity *crime* is the use of such information to obtain credit, goods, services, money, or property, or to commit a felony or misdemeanor. "Business identifying information" means a business's name, address, telephone number, corporate credit card numbers, banking account numbers, federal employer identification number (FEIN), Treasury Identification Number (TIN), State Treasury Number (TN), electronic filing identification number (EFIN: Internal Revenue Service), electronic transmitter identification number

(ETIN: Internal Revenue Service), e-business Web sites, URL addresses, and e-mail addresses.

Business identity theft has become increasingly common for three reasons.

1. Corporate credit card, bank, and other account statements generally have many more entries than the accounts of average individuals and, therefore, are more complex and less easily reconciled.
2. Corporate credit card accounts usually carry higher dollar limits than do individual accounts.
3. Many employees oftentimes are authorized to use a single corporate account. In this case, the theft and fraudulent use of the account number is less easily detected in the corporate credit card statement than in an individual credit statement, which contains fewer account entries.

Alarmingly, the theft of a business's state and federal identifiers has opened the doors to new crimes of business impersonations, such as "subsidiary" fraud. This is the registration, usually with a secretary of state, of a fraudulent subsidiary company using a legitimate business's identifiers. With the payment of a modest registration fee, in some states as little as $25, parasite subsidiary "businesses" can be formed and pose as legitimate businesses, incurring never-to-be-paid expenses for goods and services and obtaining cash through fraudulent business loans and other means. Sometimes these bogus entities defraud legitimate companies by invoicing them for services never rendered or by ordering merchandise that is then sold on the black market.

The most common personal identity crimes are credit card, bank, utilities, telecommunications, and retail (e-business and onsite) fraud. By comparison, the most common forms of business identity crimes are credit card, bank, retail account, and (of most recent origin) subsidiary fraud. These lists are growing. Increasingly, other crimes and new adaptations of crimes are being committed by using stolen identities, both personal and business—which is why the theft of an identity is, in and of itself, an all-encompassing and overarching crime.

IDENTITY THEFT AS AN "OVERARCHING" CRIME

Identity theft is the crime of the twenty-first century, because identity theft is a crime overarching and enabling many other types of crime. For example, stolen identities are used to commit credit card and bank fraud; retail account, utilities, and telecommunications fraud; mortgage and loan fraud; employment fraud; mail fraud; wire fraud; drug trafficking; money laundering; government documents and benefits fraud; prize, sweepstakes, and lottery scams; Internet auction fraud; online stalking and harassment; pornography distribution and consumption; human smuggling (women, children, and illegal immigrants); e-business fraud and a host of other cybercrimes; and terrorism.

According to federal authorities, identity theft is a key catalyst in funding terrorism.[1] Most, if not all, acts of terror against the United States are thought to have been accomplished by the use of fake or stolen identities, including the bombings of the U.S. embassies in Kenya and Tanzania, of the USS *Cole*, of the Marine Corps barracks in Lebanon, of the World Trade Center in 1993, and the atrocities of September 11, 2001. The al Qaeda training manual describes "key missions" that consist of "blasting and destroying" places of amusement, bridges into and out of cities, and embassies.[2] Not mentioned is the conversion of commercial airlines into homicidal guided missiles, although we now know that terrorists also financed these and other attacks using authentic (i.e., stolen versus fabricated) identities, impersonating real people with actual birth and credit records.

In fact, when leaving their training camps in Afghanistan or elsewhere, the "brothers" are provided five discrete sets of identities and given explicit instructions on how and when to use them. For example, when using the identity of a given individual, the impersonator is to speak the language of that individual and dress according to the custom of the individual's identity. Lesson 3 in the al Qaeda manual gives these instructions:

> The brother who has special work status (commander, communication link...) should have more than one identity card and passport. He should learn the contents of each, the nature of the

> (indicated) profession, and the dialect of the residence area listed in the document (p. 22).

In one reported case of identity theft, tens of thousands of foreigners illegally obtained Social Security numbers (SSNs) from the U.S. Social Security Administration.[3] Such an action raises cause for great concern: Once terrorists secure stolen names, addresses, Social Security numbers, and other personal identifiers, they frequently use these identifiers to create bogus passports and driver's licenses, to open bank accounts, to rent automobiles, and to otherwise cover up their nefarious activities. Extremist groups target American businesses and institutions because of the severe financial impact their terrorist acts inflict. Identity theft, therefore, is an overarching crime that enables many other crimes, including terrorism and the devastation it wreaks.

There are no national security standards in place to prevent identity thefts and the resulting wave of identity crimes. Independent businesses are ruined, and, in the aggregate, the financial infrastructure and the very security of our nation are undermined. As will be shown, the effects on people and businesses already have been devastating.

Chapter 2

IDENTITY THEFT: EFFECTS ON VICTIMS

The victims of identity theft and identity crime, respectively, are the individuals and businesses whose identities have been stolen and the individuals and businesses who are defrauded using such stolen identities. The “theft” and the “crime” are two different offenses, each with its own structure of penalties and fines. Also to be distinguished are the effects of these crimes on persons versus businesses. Both suffer the financial losses, but for persons there also is an emotional component that sometimes is so intense that even the term “identity rape” is inadequately descriptive.

EFFECTS ON PERSONS

People may be made aware that they are victims of identity theft in a number of ways, including when they:

- Receive a telephone call from the diligent fraud department of a bank, credit union, or other financial institution, inquiring about a recent credit application
- Are contacted by a collections department or agency asking why their account is delinquent
- Discover unauthorized long-distance calls on their telephone or cell phone bill
- Discover fraudulent checks deducted on their checking account statements