This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

The Role of the United States Postal Service in Public Safety and Security

Implications of Relaxing the Mailbox Monopoly

Lois M. Davis, Michael Pollard, Jeremiah Goulka,
Katherine Mack, Russell Lundberg, Paul Steinberg

Sponsored by the United States Postal Service

Safety and Justice

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

This research was sponsored by the United States Postal Service and was conducted under the auspices of the Safety and Justice Program within RAND Infrastructure, Safety, and Environment (ISE).

Library of Congress Cataloging-in-Publication Data

The role of the United States Postal Service in public safety and security : implications of relaxing the mailbox monopoly / Lois M. Davis ... [et al.].
p. cm.
ISBN 978-0-8330-4615-4 (pbk. : alk. paper)
1. United States Postal Service. 2. Postal service—United States—Safety measures. I. Davis, Lois M.

HE6371.R58 2008
363.1—dc22

2008044821

Published 2008 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

The United States Postal Service (USPS) has long held statutory monopolies to deliver mail and to require that only U.S. mail be delivered to the mailbox. While the USPS has defended its monopolies as necessary to fulfill its mission to provide service to every delivery point in the United States, several critics have argued against the monopolies, primarily on economic, antimonopoly grounds related to leveling the playing field for other competitors and on property rights grounds for mailbox owners. However, sometimes lost in the economic debate surrounding the monopolies is the fact that relaxing the monopolies may have ramifications in other areas—in particular, public safety and security. When it comes to delivering mail, there are several possible public safety and security concerns, including, for example, mail fraud, identity theft, and even terrorism, as demonstrated by prior use of the mail to send letter bombs and anthrax.

Given the potential public safety and security concerns, the USPS asked the RAND Corporation to assess the security implications of relaxing the USPS's monopoly on delivering to the mailbox (known variously as the *Mailbox Restriction*, the *Mailbox Rule*, or the *Mailbox Monopoly*) to allow private couriers to deliver directly to mailboxes as well. Specifically, the project addresses whether relaxing the Mailbox Rule would present a public safety risk to carriers, couriers, and customers. To do so, RAND researchers used a combination of qualitative analyses (e.g., literature review, key-actor interviews with USPS staff and external experts, and a survey of consumers) and descriptive quantitative analyses (e.g., of incident databases collected by the United

States Postal Inspection Service, or IS). However, it is important to note that all of our statements with regard to private couriers and comparisons to the USPS are based solely on publicly available documents and some suggestive data from the IS incident database. Without other detailed, direct information from the couriers, similar to that provided by the USPS, we can only infer what their current capacity is for managing safety and security issues in the processing and delivery process.

This research should be of interest to policymakers, Congress, and the private sector.

The RAND Safety and Justice Program

This research was conducted under the auspices of the Safety and Justice Program within RAND Infrastructure, Safety, and Environment (ISE). The mission of RAND Infrastructure, Safety, and Environment is to improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Safety and Justice Program research addresses occupational safety, transportation safety, food safety, and public safety—including violence, policing, corrections, substance abuse, and public integrity.

Questions or comments about this monograph should be sent to the project leader, Lois Davis (Lois_Davis@rand.org). Information about the Safety and Justice Program is available online (http://www.rand.org/ise/safety). Inquiries about research projects should be sent to the following address:

Greg Ridgeway, Acting Director
Safety and Justice Program, ISE
RAND Corporation
1776 Main Street
Santa Monica, CA 90407-2138
310-393-0411, x7734
Greg_Ridgeway@rand.org

Contents

Figures

Tables

Summary

Introduction

The United States Postal Service (USPS) has long held statutory monopolies to deliver mail (the *Postal Monopoly*) and to have sole access in delivering mail to the mailbox (referred to as the *Mailbox Restriction*, *Mailbox Rule*, or *Mailbox Monopoly*). These monopolies were created to protect USPS revenue to enable it to fulfill its universal service obligation (USO)—its obligation to provide service to every delivery point in the United States. However, several critics have argued against the monopolies, primarily on economic, antimonopoly grounds related to leveling the playing field for other competitors and on property rights grounds for mailbox owners. The debate surrounding the monopolies focuses primarily on economic issues, but relaxing the monopolies may have ramifications in other areas—in particular, public safety and security. Given the potential public safety and security concerns, the USPS asked the RAND Corporation to assess the security implications of relaxing the Mailbox Rule; such relaxation would allow private courier companies or individuals to deliver items directly to the mailbox.

The Mailbox Rule stems from a criminal statute that Congress passed in 1934 (18 U.S.C. § 1725) to protect postal revenue when utilities and other companies began to distribute bills directly to customers. While the statute does not actually make it illegal for non-USPS employees to deliver mail, it does make it a crime to deliver mail without postage to a mailbox. The Mailbox Rule has two primary policy effects. First, it prevents private courier companies from making their deliveries to the mailbox. These deliveries must instead

be handed directly to their recipients or deposited, for example, on a home's front step. Second, it indirectly adds to the scope of the Postal Monopoly. The Postal Monopoly was first created by the Postal Act of 1845 and is shaped largely by the Private Express Statutes (PES) and Postal Accountability and Enhancement Act of 2006 (PAEA), which, with their implementing regulations, provide the USPS with sole authority to deliver "letters and packets" and many other types of mail. What they do not cover may be delivered either by the USPS or by private couriers, but the Mailbox Rule makes it too expensive for private courier companies to separate mailbox addresses from nonmailbox addresses (e.g., mail slots, company mailrooms).

This monograph analyzes the possible public safety and security ramifications of altering the Mailbox Rule. What public safety and security effects might occur if more people and organizations were involved in making deliveries to the mailbox? What might occur from a public safety and security perspective if some amount of USPS mailflow were diverted to other couriers? It is important to note that there is no consensus about whether the Mailbox Rule should be relaxed or what a relaxation might look like. Possibilities for relaxation might include allowing major existing private courier companies to deliver to the mailbox, creating a licensing regime to allow additional companies to deliver, or generally opening the mailbox to private deliveries. Any scenario would likely include a de facto continuation of the USPS monopoly over locked mailboxes (such as those found in apartment buildings and some neighborhoods), simply because locked mailboxes would require their own rules due to logistical and security issues connected to the possession of mailbox keys. Further, there would be significant costs involved in converting locked mailboxes to unlocked mailboxes or in managing mailbox keys to give legitimate couriers access to locked mailboxes.

In analyzing the security repercussions of relaxing the monopolies, we report on three sets of analyses: (1) assessing the relaxation's potential impact on public security and safety incidents; (2) assessing its impact on the ability of the United States Postal Inspection Service (IS) to detect, deter, and investigate mail crimes; and (3) assessing the public's perceptions of the Mailbox Rule and concerns about relaxing

it. To perform these analyses, this study used a combination of qualitative analyses (e.g., literature review, key-actor interviews, and a survey of consumers) and descriptive quantitative analyses (e.g., secondary data analysis of incident databases collected by the IS).

This study was bounded by several limitations. First, we were not asked to consider the public safety and security issues connected with relaxing the Postal Monopoly generally—only the relaxation of the Mailbox Rule. We also did not consider the economic ramifications of relaxing the USPS monopolies. Second, we had minimal data from private courier companies to compare with USPS practices. We attempted to interview several of the major U.S. private courier companies but did not receive a response to our requests; thus, we relied on publicly available corporate documents about the training and safety and security measures these companies have undertaken, as well as on analyses of the IS reported-incident databases. Without other direct information from private couriers, similar to what the USPS provided, we can only infer what their current capacity is for managing safety and security issues in processing and delivery. Third, we provide a broad overview of the range of USPS training and guidance; we did not comprehensively analyze all training and guidance, nor did we evaluate the quality of the training provided. Fourth, the IS reported-incident databases reflect detected and reported incidents, which means it is impossible to distinguish for certain whether changes over time reflect actual increases in incidence or increased detection or reporting. The true number of all these incidents is unknown. Finally, because we did not have incident data from other countries, our assessment of other countries' experience of relaxing their postal monopolies relied on a qualitative assessment.

Impact of Relaxing the Mailbox Rule: Public Safety and Security Incidents

Based on our descriptive analysis of the reported-incident databases (which identified security-related incidents by urban/rural splits and household income) and in conjunction with our assessments of key

differences in training, accountability, and oversight between the USPS and private couriers, we expect that several effects on security would result from relaxing the Mailbox Rule. If access to the mailbox is opened up to deliveries other than U.S. mail, the main risk to the public may be in terms of theft from the mailbox. Mail theft plays a role in many broader crimes—including, for instance, identity theft and the fraudulent use of stolen credit cards, pension checks, or other payments. An increase in mail theft might occur because more people would make deliveries to the mailbox, increasing opportunities for mail theft. In addition, depending on how the Mailbox Rule is relaxed, we would expect greater variability in personnel in terms of the type of training that personnel have received. This suggests that the training costs and need for additional training of USPS and IS personnel will likely increase.

Depending on the actual amount of U.S. mail volume that shifts to private couriers and the number of carriers involved in deliveries, security and safety may also decrease in other ways. In our view, mail-related financial crimes and explosives-related incidents may increase, as might the delivery of suspicious items (that might cause harm or fright) to consumers due to differences in training and in the number of personnel delivering to the mailbox. Further, training on the USPS side will likely have to increase to deal with the variability of events happening at the point of delivery. It is difficult to assess the current baseline level of risk from which these increases will occur. For instance, while the IS databases identify real safety and security concerns, the true extent of financial crime is unknown. (The nature of IS data collection likely underestimates the true level of crime substantially.)

These changes raise a fundamental question of whether training standards should be set as part of any decision to open access to the mailbox and, if so, who will be responsible for enforcing those standards.

Finally, opening up access to the mailbox may create two tiers of public safety, with rural and lower-income areas being *less likely* to experience the diversion of mail to private couriers due to private couriers potentially "cream-skimming" urban and higher-income areas.

Impact of Relaxing the Mailbox Rule: The IS's Ability to Detect, Deter, and Investigate Crime

Based on an assessment of the limited available data and of USPS arguments, we find that relaxing the Mailbox Rule would limit the number of crimes that the IS polices, which would deny the public the benefit of the only law enforcement agency that specializes in this field. Relaxing the Mailbox Rule would also make it more complicated and costly for the IS to police the crimes that would remain in its jurisdiction.

In discussions with the IS, one concern we heard was that the increased cost and complexity of investigations involving the mailbox would force the USPS to terminate its jurisdiction over mailboxes and crimes that occur in them. However, our analysis suggests that the USPS may not be forced to take this action, at least for U.S. mail delivered to the mailbox; nonetheless, the cost increase in maintaining jurisdiction over the mailbox could be significant.

We agree with the IS that relaxing the Mailbox Rule would limit federal jurisdiction over deliveries that are diverted to private couriers. Except for the mail-crime statutes that include a provision for federal jurisdiction based on interstate commerce, these statutes do not apply to private courier companies, because their deliveries are not "mail." Even if Congress were to add provisions for federal jurisdiction based on interstate commerce to the remainder of mail-crime statutes, doing so would not address *intrastate* crimes. Furthermore, because the IS has investigative jurisdiction only over crimes involving U.S. mail, it would not be the agency charged with investigating crimes involving private courier companies, even when federal jurisdiction exists.

Relaxing the Mailbox Rule would increase the cost and complexity of IS investigations for several reasons. The IS would have to confirm that the crime involved a USPS delivery; investigations involving mailbox surveillance would have to deal with more suspects; and the IS would have more jurisdictional and territorial issues to address in each investigation. Relaxing the Mailbox Rule would also reduce the IS's visibility into national mail-crime trends because it would shrink the amount and consistency of information available.

Finally, although the Mailbox Rule generally has negligible deterrent effect against crime, it is possible that any deterrence gained from the strategic focus of IS resources—such as mass mail theft—will be lost. This would be the result of the shrinkage of IS investigative jurisdiction caused by the diversion of mail to private couriers and the possible cancellation of the mailbox's status as an "authorized depository" of mail, as well as the occasional lack of parallel state or local prohibitions or regulatory systems for postal crimes.

Several of these negative impacts could be somewhat mitigated. Congress could mandate that the mailbox remain an authorized depository of mail for the purposes of federal jurisdiction over crimes against U.S. mail in the mailbox and against the mailbox itself (but not crimes against private courier deliveries to the mailbox, such as theft or tampering). An appropriation might be necessary to enable continuing jurisdiction over the mailbox. Congress could add an interstate commerce basis for federal jurisdiction to the remainder of mail-crime statutes that currently rely only on the mail for federal jurisdiction, such as sending explosive devices, nonmailable hazardous materials, and firearms. However, extending the IS's investigative jurisdiction to deliveries that are diverted to private courier companies would place the IS in the uncomfortable position of policing the USPS's competition. A national reporting requirement could partially mitigate the problem of visibility caused by diversion, even if it applied to law enforcement agencies rather than private courier companies, but it would likely require additional funding. Through a direct appropriation, Congress could mitigate the additional resource burdens that relaxing the Mailbox Rule would place on IS investigations. Alternatively, some increased costs might be offset, at least in part, by the reduction in the IS's caseload because of the shrinkage of its investigative jurisdiction.

Public Perceptions About Relaxing the Mailbox Rule

To determine what the public thinks about relaxing the Mailbox Rule, we conducted a survey using RAND's established, nationally representative American Life Panel (ALP) to complement and expand on exist-

ing surveys. Overall, we found that a majority of respondents favored keeping the Mailbox Rule in place; however, a third were in favor of extending access to trusted courier companies. When individuals were given more information about the implications of relaxing the Mailbox Rule, they were less likely to support extending access. These results are consistent with the U.S. Government Accountability Office's (GAO) 1994 survey suggesting that the opposition to opening up mailbox access has remained consistent for at least the past 15 years (GAO, 1997).

Security and identity-theft concerns are important factors underlying respondents' concerns about relaxing the Mailbox Rule. Most respondents cited security-related reasons as their strongest ones for opposing increased access. In general, the more concerned individuals were about security, the more likely they were to favor restricting access to their mailboxes.

Finally, there is some evidence that opening up mailbox access is more acceptable to those whom it will most affect. Specifically, rural households are less likely to be affected by removing the Mailbox Rule. Yet, rural households were more likely than urban households to oppose removing the Mailbox Rule. To some extent, this difference may derive from urban households' comfort with private couriers. We expect that rural households are less likely than urban households to interact with private couriers on a regular basis (either because of less frequent courier deliveries to rural areas or because of the USPS's "last mile" delivery service for some courier-service items[1]). This level of comfort among urban households could alleviate their concerns about private couriers. If access were granted to private couriers, it is unclear whether public

[1] Last mile deliveries are made in cases in which private courier companies use the reach of the USPS delivery network. A private courier service delivers an item as far into its own delivery network as it can, then contracts with the USPS to deliver the item to a location beyond that point where it is more logistically and cost effective to use the USPS delivery network. For example, the USPS has provided last mile delivery for DHL since 2003 in more than 20,000 ZIP Codes nationwide through its Parcel Select service; the USPS is the exclusive provider of delivery service to DHL for 3,600 of the nation's 46,000 ZIP Codes through use of Priority Mail and Parcel Select service (USPS, 2008c).

opinion would shift over time as rural households become more familiar and comfortable with these couriers.

Issues to Consider If the Mailbox Rule Is Relaxed

Overall, we expect that relaxing the Mailbox Rule will have a negative effect on public safety and mail security, as well as increase the number of mail crimes that are not reported, although we speculate that the magnitude of the impact on incidents (based on the limited data available) would likely be moderate. Such an impact would be contingent on the degree of relaxation, particularly whether only the major couriers or a range of different types of couriers are allowed to enter the postal market. Whatever the degree of relaxation may be, there is a stronger case for predicting an increase in the cost and complexity of IS investigations. If Congress decides to explore the possibility of relaxing the Mailbox Rule, a number of issues will need to be addressed. Although we point to where there may be increases in the number of incidents, training requirements and costs, and investigation costs and investigative complexity, it is not possible to quantify the magnitude of increases in these areas without a clear set of options against which to evaluate such increases and more data regarding private courier company practices.

That said, we highlight issues that should be considered to help mitigate the public safety and security impacts that might occur if the Mailbox Rule were relaxed.

- Congress may want to consider options for establishing national training standards for private couriers and identify what agency will be responsible for oversight and enforcement of those standards. If the USPS is given a role in training private couriers to national standards, such an increase in responsibilities would need to entail a corresponding increase in funding.
- A national reporting system may need to be established to allow the IS and the U.S. Department of Justice (DOJ) to continue

to track mail crime and crime involving private couriers and to assess mail-crime trends over time.

- With respect to the issue of federal jurisdiction over the mailbox, Congress may want to consider mandating that the mailbox remain an authorized depository of mail for the purpose of USPS deliveries.
- To somewhat mitigate the loss of federal jurisdiction over mail crime because of diversion of mail to private couriers, Congress may want to increase the number of mail-crime statutes that have an interstate commerce hook. Congress should decide which federal law enforcement agency has investigative jurisdiction over those crimes, as it may be inappropriate for the IS to investigate interstate crimes involving private courier companies that compete with the USPS.
- To address consumers' concerns about security and implications of relaxing the Mailbox Rule, public education and awareness campaigns may need to be implemented to inform consumers about what will change and what that will mean for them (e.g., to whom they will report mail crime, how they will know whether a courier is legitimate). The public awareness campaigns would need to be tailored to address the needs of different populations—for example, for rural populations—who may be more resistant to the change.
- Finally, if there is a strong political will to relax the Mailbox Rule, one option for collecting data in order to quantify the potential impact on public safety and security, as well as other issues, would be to undertake a pilot project in a limited number of areas that would allow individuals to give select parties access to their mailbox. If such a pilot is undertaken, data should be collected on each reported incident (including type of incident), what carrier was involved, characteristics of the incident, to whom the consumer reported the incident, who the responder was, and investigation costs. Doing so would be important to quantify the hypothesized impact that relaxing the Mailbox Rule may have on public safety and mail crime. Having such information would, in turn, be cru-

cial in determining the soundness of relaxing the Mailbox Rule and in designing a national implementation.

Acknowledgments

The authors would like to thank Scott J. Davis, Kimberly A. Weaver, and Tina D. Gupta of the USPS for their guidance and for providing documents and other data sources needed for this study. We also wish to thank Bruce R. Reiter for providing the incident data used in this analysis. In addition, we would like to thank John Allen, Chief Executive of New Zealand Post Group, and John Caines, Manager of National Media Relations, Canada Post, for their thoughtful comments and input on this monograph.

We also appreciate the insights provided by our technical reviewers—Susan Turner of the University of California, Irvine, and RAND and Robert W. Taylor of the University of North Texas—who reviewed and commented on drafts of this monograph.

Of course, any errors or omissions are the sole responsibility of the authors.

Abbreviations

ALP	American Life Panel
AMF	Airport Mail Facility
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
ATM	automated teller machine
BDS	Biohazard Detection System
CBP	U.S. Customs and Border Protection
CBU	cluster-box unit
CDC	Centers for Disease Control and Prevention
CHSP	Comprehensive Health and Safety Process
CID	Criminal Investigation Command
COA	change of address
CRI	Cities Readiness Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	U.S. Department of Homeland Security
DMI	dangerous-mail investigation
DMM	Domestic Mail Manual

DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
EAP	emergency action plan
EMS	emergency medical services
ESF	Emergency Support Function
FAA	Federal Aviation Administration
FCD	Financial Crime Database
FCS	Fraud Complaint System
FTC	Federal Trade Commission
GAO	U.S. Government Accountability Office (U.S. General Accounting Office prior to July 7, 2004)
HAZWOPER	hazardous-waste operations and emergency response
IED	improvised explosive device
IEMP	Integrated Emergency Management Plan
IS	United States Postal Inspection Service
JSA	job-safety analysis
JTTF	Joint Terrorism Task Force
MICT	mail isolation, control, and tracking
NALC	National Association of Letter Carriers
NDCBU	neighborhood delivery and collection-box unit
NIPP	National Infrastructure Protection Plan
NRF	National Response Framework
NTD	National Training Database

OIG	United States Postal Service Office of Inspector General
OSHA	Occupational Safety and Health Administration
OSI	Office of Special Investigations
P&DC	Processing and Distribution Center
PAEA	Postal Accountability and Enhancement Act of 2006
PEG	Performance Evaluation Guide
PES	Private Express Statutes
POD	Point of Dispensing
PPE	personal protective equipment
PPO	Postal Police Officer
PRC	Postal Regulatory Commission
SCBA	self-contained breathing apparatus
SCO	Security Control Officer
SIRS	Suspicious Incident Reporting System
SLAP	shape, look, address, or packaging
TRAC	Transactional Records Access Clearinghouse
TSA	Transportation Security Administration
UPS	United Parcel Service of America, Inc.
USO	universal service obligation
USPS	United States Postal Service
VFS	Ventilation and Filtration System

CHAPTER ONE

Introduction

Background

The United States Postal Service (USPS) has long held statutory monopolies to deliver mail and to have sole access to delivering to the mailbox. While the USPS has defended its monopolies as necessary to fulfill its mission to provide service to every delivery point in the United States, several critics have argued against the monopolies, primarily on economic, antimonopoly grounds related to leveling the playing field for other competitors and on property rights grounds for mailbox owners (see, e.g., Geddes, 2003a, 2003b; Sidak, 2003; Soifer et al., 2007).

However, sometimes lost in the economic debate surrounding the monopolies is the fact that relaxing the monopolies may have ramifications in other areas—in particular, public safety and security. When it comes to delivering mail, there are several significant public safety and security concerns—including, for example, mail fraud, identify theft, and even terrorism, given the previous use of the mail to send letter bombs and anthrax.

Given the potential public safety and security concerns, the USPS asked the RAND Corporation to assess the security implications of relaxing its monopoly on delivering to the mailbox (known as the *Mailbox Restriction*, *Mailbox Rule*, or *Mailbox Monopoly*)[1] to allow courier companies to deliver directly to the mailbox. More specifically, the

[1] We use the name *Mailbox Rule*; the reader should not confuse this with either the Postal Monopoly (the USPS monopoly on delivering mail) or the contract law concept that is also called the Mailbox Rule.

project addresses whether relaxing the Mailbox Rule would present a public safety risk to carriers, couriers, or customers.

The study scope focused specifically on examining the public safety and security issues related to any proposal to relax the Mailbox Rule.[2] The USPS has contracted separately for a study to examine the financial implications of doing so. As such, we only note in this monograph where our analyses suggest that there may be some cost implications (e.g., investigation costs related to the relaxation of the Mailbox Rules).

Study Approach

To accomplish our objective, we used a combination of qualitative analyses (e.g., literature review, key-actor interviews, and a survey of consumers) and descriptive quantitative analyses (e.g., secondary data analysis of reported-incident databases maintained by the United States Postal Inspection Service, or IS).

In applying this overall approach, we conducted five tasks: (1) evaluate what public safety and security training is undertaken by the USPS and how that compares with that provided by private couriers as a way to assess the risks that untrained couriers, as well as USPS mail carriers, may face if the Mailbox Rule is relaxed; (2) review the existing literature and conduct a short survey and then summarize what is known about the public's concerns about mail security, its experience with crimes associated with the mailbox, and its views about different types of proposed access to the mailbox by non-USPS entities; (3) analyze the IS database, tabulating and describing the kinds of reported crimes that occur with the current monopolies in place and then making projections on how much certain types of crimes may increase from this baseline if the Mailbox Rule is relaxed; (4) assess whether proposals to relax the Mailbox Rule may inhibit the effective

[2] Chapter Two explains the contours of the Mailbox Rule and the USPS monopoly on delivering mail (the *Postal Monopoly*). Because relaxing the Mailbox Rule would involve a partial relaxation of the Postal Monopoly, part of this monograph's analysis logically extends to the general relaxation of the Postal Monopoly.

investigation and prosecution of serious crimes by examining federal criminal laws to determine how federal criminal jurisdiction would be affected by relaxing the Mailbox Rule; and (5) examine the experience of other countries—in particular, the United Kingdom, Canada, and New Zealand—in opening up their postal markets to competition, with the goal of capturing lessons learned with respect to public safety and mail security. The results of these tasks are incorporated into the findings in the subsequent chapters.

Study Limitations

This study is bounded by several limitations. As noted, we were not asked to consider the public safety and security issues connected to relaxing the Postal Monopoly generally. However, we do discuss issues related to its relaxation to the extent that it is predicated on the Mailbox Rule. Neither did we consider the economic ramifications of relaxing either of the USPS monopolies.

More specifically and related to the analyses themselves, we had very little data on private courier companies to compare with data on USPS practices. We attempted to interview several of the major private courier companies operating in the United States to learn firsthand about the training, guidance, policies, procedures, and technology they currently use to protect the safety and security of their employees, their deliveries, and their customers. However, because we did not receive a response to our requests, we were limited to publicly available corporate documents about the training and safety and security measures that these companies have undertaken, as well as on analyses of the IS reported-incident databases.

In addition, although we provide a broad overview of the range of USPS training and guidance, we did not comprehensively analyze all training and guidance; thus, the summary provided in the document should not be viewed as an exhaustive list. Further, we did not evaluate the quality of the training provided; rather, our focus was on assessing what type of training and public safety and security precautions are taken to safeguard the mail, postal employees, and customers. In addi-

tion, because this monograph focuses primarily on the public safety and security implications of opening up access to the mailbox, we did not examine training related to aviation security. Finally, in considering the role of private couriers, we did not examine in any depth what regulations may apply to these companies.

As noted, one part of our research involved analyzing the IS incident databases. It is important to note that all these databases reflect detected or reported incidents. It is impossible to distinguish with any certainty whether changes over time reflect actual increases in incidence or increased detection or reporting. The actual number of all these incidents is unknown.

For instance (as we discuss later), the financial crime data suggest that 1.1 percent of the population was victimized by a reported financial crime through the postal system annually in 2006 or 2007. This number is far lower than other estimates of the number of crimes (e.g., the Better Business Bureau's 2005 survey indicated that 4 percent of the age 16+ population were victims of identity theft in 2004 alone); then again, many of these other complaints may never have been reported to the USPS. It is important to note that, like most crime reporting, the fraud data and financial crime data include only incidents that were reported to the USPS (by customers, financial institutions, companies, or other law enforcement agencies). Therefore, the true level of fraud and financial crime occurring cannot be obtained from these data (only the number of reports for each type of incident).

Also, the "suspicious incident" data are virtually all "false positives," including the incidents involving explicit threats (hoaxes), complicating the interpretation of the results. Detected leaking liquid items, for example, may not represent an actual physical threat, but such leakage could have damaged other items in the postal system. Hoaxes, while typically not physically dangerous, can instill fear and are often deemed criminal acts.

Finally, we cite examples in which the experience of other countries in opening up their postal monopolies may shed some light on public safety and security concerns for consideration for the United States. However, such comparisons are limited by differences in characteristics and size of their postal markets, and in the mix of residential

mail receptacles used (GAO, 1997).[3] In addition, incident data were not available from other countries, which would have allowed us to compare trends for before and after they relaxed their postal monopolies. As a result, representatives of these postal services were able to provide only a qualitative assessment about the effects of relaxing their postal monopolies on detection of mail crime and investigations.

Organization of This Monograph

We organized this monograph as follows. Chapter Two provides some context for the chapters that follow. In particular, it examines the two monopolies in more detail and what would happen in broad, non–security-related terms if the Mailbox Rule were to be relaxed. The chapter also provides an overview of the USPS role in security and public safety, as well as the role of the major private couriers.

Chapters Three and Four focus on the public safety and security implications that relaxing the Mailbox Rule might have on the USPS's ability to prevent the occurrence of security incidents and to detect, deter, and investigate security incidents that do occur, respectively. In Chapter Three, we first present the results of our descriptive analyses of the IS incident data to describe the kinds of reported crimes that occur with the current monopolies in place. Next, we argue which types of incidents may increase if the Mailbox Rule were to be relaxed, along with our arguments for why such increases may occur, based on an examination of USPS training, oversight, and accountability. Chapter Four looks at the impact that relaxing the Mailbox Rule could have on the IS's ability to conduct effective investigations and prosecutions of crimes. We also note in each chapter where other countries' experiences may provide some insights or help highlight public safety and mail security issues that need to be considered.

---

[3] For example, of eight foreign postal administrations surveyed by the GAO (1997), two countries reported that the majority of their residents used mail slots in doors or walls, and another country reported the use of a higher proportion of locked mailboxes than are used in the United States.

Chapter Five summarizes the results of literature reviews and a national survey conducted to examine the public's concerns about security, its experience with crimes associated with the mailbox, and its views about different types of proposed access to the mailbox by non-USPS entities.

Finally, Chapter Six provides some conclusions based on our analytic findings and discusses some issues to consider if the Mailbox Rule is relaxed.

Appendix A discusses in more detail our methods and approaches, while Appendix B provides more-detailed tabular displays from our analysis of the IS incident databases. Appendix C provides a detailed list of USPS employee guidance and training. Finally, Appendix D summarizes differences between Federal Trade Commission (FTC) data and IS data on consumer fraud.

CHAPTER TWO

The USPS's Monopolies and Its Role in Public Safety

In this chapter, we provide some context that will help explain the results that follow in the subsequent chapters. Although the focus of this monograph is on the Mailbox Rule (as noted in Chapter One), it is important to have a general understanding of the two statutory postal monopolies—the Mailbox Rule and the Postal Monopoly—and how they are related. Following a discussion of these two monopolies, as a prelude to discussing the security and public safety repercussions in Chapters Three and Four, we discuss what would happen if the Mailbox Rule were to be relaxed. Finally, we provide an overview of the current USPS and IS roles in public safety and security and contrast those roles with those of the private couriers.

Introduction to the USPS Monopolies

The USPS has two major monopolies over mail service in the United States. Both monopolies were created to financially enable the USPS to fulfill one of its primary responsibilities—its universal service obligation (USO). Unlike private courier companies and services, the USPS is *required* to deliver to all of the approximately 148 million mail delivery points across the United States, six days per week, from the areas with the highest rates of crime to the bottom of the Grand Canyon (USPS, 2008d, p. 32; USPS, 2008a).

The Mailbox Rule

The focus of this monograph is the USPS's monopoly access to the mailbox, known as the *Mailbox Rule*. It is this rule that prevents private couriers from delivering to the mailbox and to Post Office Boxes. Instead, private couriers must make their deliveries to the door, doorstep, doormat, doorpost, or some place other than the mailbox itself.

Congress created the Mailbox Rule in 1934 to protect USPS revenue. Fearing that utility companies were threatening the USPS's ability to meet its USO by delivering bills and circulars directly to its customers, Congress made it a federal crime, punishable by fine, to deliver to the mailbox any mailable materials without postage.

> Whoever knowingly and willfully deposits any mailable matter such as statements of accounts, circulars, sale bills, or other like matter, on which no postage has been paid, in any letter box established, approved, or accepted by the Postal Service for the receipt or delivery of mail matter on any mail route with intent to avoid payment of lawful postage thereon, shall for each such offense be fined under this title. (18 U.S.C. § 1725, as amended)

Through its own regulations, the USPS has extended the Mailbox Rule to "every letterbox or other receptacle intended or used for the receipt or delivery of mail on any city delivery route, rural delivery route, highway contract route, or other mail route," designating them as "an authorized depository for mail" for several federal crimes (DMM 508.3.1.1),[1] as well as to "items or matter placed upon, supported by, attached to, hung from, or inserted into a mail receptacle" (DMM 508.3.1.3). It is important to note that this rule applies to both locked and unlocked mail boxes, as well as to Post Office Boxes. It does not, however, apply to mail slots in front doors, because the USPS has no access beyond the mail slot (an issue we discuss in more detail in Chapter Four). The general theory is that a USPS customer limits the possible uses of his or her mailbox in exchange for USPS business services (such as sending outgoing mail or leaving cash to buy stamps)

---

[1] The Domestic Mail Manual (DMM) has been incorporated as valid administrative regulation by reference in 39 Code of Federal Regulations § 111.

and USPS security services (including federal criminal investigations and prosecutions).

The U.S. Supreme Court upheld the constitutionality of the Mailbox Rule in *United States Postal Service v Greenburgh Civic Associations* in 1981 (453 U.S. 114), although the case addressed only a First Amendment challenge raised by issuers of circulars. The Court held that the Mailbox Rule was not intended to limit speech but instead to affect everyone equally. The case did not involve any competition or property rights challenges to the Mailbox Rule. Courts have since assumed the rule's legality.

The Postal Monopoly

The USPS's more widely known monopoly is that over mail, known as the *Postal Monopoly*. This was first created by the Postal Act of 1845 and subsequently shaped by a set of civil and criminal statutes known collectively as the Private Express Statutes (PES) as well as the Postal Accountability and Enhancement Act of 2006 (PAEA).[2] As the President's Commission on the United States Postal Service noted, there is no "straightforward" definition of the Postal Monopoly, and, since many of its provisions are rooted in now obsolete conveyances, the PES are confusing to the modern reader (President's Commission on the United States Postal Service, 2003, p. 22).

These statutes provide the USPS with sole authority to deliver "letters and packets." Because packets are largely obsolete,[3] the definition of *letter* creates much of the Postal Monopoly: "a message directed to a specific person or address and recorded in or on a tangible object" (39 C.F.R. § 310.1(a)).[4]

---

[2] 18 U.S.C. §§ 1693–1699, 39 U.S.C. §§ 601–606, 39 C.F.R. § 310.3(a) *et seq*., and implementing sections of the DMM. For an in-depth analysis of the PES and the PAEA as they relate to the Mailbox Rule, see USPS (2008d). For a thorough discussion of the PES prior to passage of the PAEA, see GAO (1997) and Craig and Alvis (1977).

[3] Packets are "two or more letters, identical or different, or two or more packets of letters, under one cover or otherwise bound together" (18 U.S.C. § 1694; 39 C.F.R. § 310.1(b)).

[4] The USPS lists the following exceptions to the definition of a *letter*:

> telegrams, financial instruments sent between financial institutions, certain legal papers, newspapers and periodicals, books and catalogs exceeding certain page limits, telephone

The PES, their regulations, and the PAEA provide several categories of mail that are not subject to the Postal Monopoly. The PAEA allows private couriers to deliver letters that weigh more than 12.5 ounces, letters carried for six times the present price for the first ounce of a single-piece First-Class Mail letter, or letters that fall under the six suspensions to the PES promulgated by USPS regulations (39 U.S.C. § 601(b)(1)–(3)). These include

- extremely urgent letters
- certain data-processing materials
- letters of bona fide college and university organizations
- international ocean carrier–related documents
- advertisements accompanying parcels or periodicals
- international remailing.

The exception for extremely urgent letters allows companies like FedEx, UPS, and DHL to make their deliveries.

There are also five general exceptions to the PES.[5] The most pertinent of these are the exceptions for hand delivery without fee, transmission by "special messenger" (which allow bicycle-messenger deliveries), and "carriage prior or subsequent to mailing," which allows private companies to compete with the USPS upstream on a work-share basis by substituting private sorting and transportation such that mail enters the mail stream closer to the point of delivery (FTC, 2007, p. 15).

> directories, matter sent from a printer to its customers, letters sent for records storage, tags and other labels primarily intended to be attached to other objects for reading, photographic material between a customer and a processor, copy sent to or from a printer or compositor, audiovisual media or packets of identical printed letters for public dissemination, and computer programs designed for direct input. (USPS, 2008d, citing 39 C.F.R. § 310.1(a)(7))

[5] The five general exceptions are (1) letters or packets that "relate to some part of the cargo of such conveyance"; (2) those that "relate to . . . the current business of the carrier, or to some article carried at the same time as such conveyance"; (3) "receiving and delivering to the nearest post office, postal car, or other authorized depository for mail matter any mail matter properly stamped"; (4) "the conveyance or transmission of letters or packets by private hands without compensation"; and (5) "the conveyance or transmission of letters or packets . . . by special messenger employed for the particular occasion only," including "carriage prior or subsequent to mailing." See 18 U.S.C. §§ 1694, 1696(a),(c); 39 C.F.R. § 310.3(a)–(e).

For this study, it was essential to recognize that the Mailbox Rule effectively widens the Postal Monopoly. Although the PAEA, the PES, and their implementing regulations provide exceptions and suspensions to the Postal Monopoly, the Mailbox Rule requires postage on deliveries to the mailbox. Therefore, private couriers may not make their deliveries to the mailbox. Additionally, since all mailable "matter" in a mailbox must bear postage (and nonmailable matter may not be put there at all), companies face a choice of sending matter not covered by the PES privately to the doorstep or through the USPS to the mailbox.[6]

What Happens If the Mailbox Rule Is Relaxed?

In recent years, some policy analysts have argued that the USPS monopolies are inappropriate (see, for example, Geddes, 2003a, 2003b; Sidak, 2003; Soifer et al., 2007). Their arguments are rooted in property rights theory and free-market theory's hostility to monopolies. According to one argument, mailbox owners should be free to make their own choices about who may make deliveries to their mailboxes (for example, Soifer et al., 2007). According to another, the USPS should fully compete with private couriers (see, e.g., Geddes, 2003a, 2003b; Sidak, 2003). This argument emphasizes its status as an independent government corporation rather than a typical government department.[7]

These arguments have prompted analysis by the GAO (1997), the President's Commission on the United States Postal Service (2003), and the Federal Trade Commission (FTC, 2007), focused largely on questions of competition, modernization, and public attitudes. Their

---

[6] As an FTC report noted,

> Because the mailbox monopoly requires all 'matter' in a mailbox—not merely matter covered by the PES—to bear postage, it effectively expands the postal monopoly by increasing the cost and/or reducing the quality of non-USPS delivery of matter that legally may be carried outside of the mail. (FTC, 2007, p. 17)

[7] The Postal Reorganization Act of 1970 transformed the cabinet-level Post Office Department into an independent establishment of the executive branch named the United States Postal Service (see 39 U.S.C. § 201).

reports discuss several elements of the USPS monopolies, with particular attention to maintaining the USPS's financial ability to meet its USO.[8] The President's Commission on the United States Postal Service (2003, p. 26) recommended that a postal regulatory board be created with authority to regulate the monopolies. Concerning the Mailbox Rule, the commission recommended that the proposed board "be authorized to permit mailbox access by private carriers in future regulations, so long as it does not impair universal service or open homeowners' mailboxes against their will."

If the Mailbox Rule were to be relaxed, it is not entirely clear how it would look. Various approaches have been suggested, including a general relaxation that would allow anyone to make deliveries to any mailbox,[9] a licensing system that would allow only licensed couriers to deliver to the mailbox, and a relaxation limited to the existing major courier companies, such as FedEx, UPS, and DHL. If the Mailbox Rule were to be relaxed generally, there is a question about the effect it would have on locked mailboxes. A likely outcome would be a de facto continuation of the USPS monopoly over locked mailboxes, simply because giving keys to private courier companies would be logistically complex and politically unappealing to owners of locked mailboxes. In addition, there would be significant costs involved in converting locked mailboxes to unlocked mailboxes or in managing mailbox keys to give legitimate couriers access to locked mailboxes.

These arguments also raise the question of what would happen if the Mailbox Rule were to be relaxed. The USPS contends that relaxing the rule would likely divert a significant number of deliveries from the USPS to private courier companies because private couriers would be able to deliver items that are excepted from the PES to the mailbox. To predict the percentage of USPS mail-flow that would be at risk of diversion to private couriers, the USPS has commissioned a separate study that is currently in process.

---

[8] To put this concern in context, the USPS has experienced a multibillion-dollar loss in fiscal year (FY) 2008 and expects a multibillion-dollar loss in FYs 2009 and 2010 as well.

[9] Currently, anyone *can* deliver to the mailbox, as long as the matter delivered has proper postage.

However, to very roughly estimate the percentage of mail-flow at risk of diversion, the USPS notes that mail that is excepted from the PES is delivered through the following USPS services: Priority Mail; First-Class Mail parcels; Small Parcel Post, Bound Printed Matter, and Media Mail parcels; Standard Mail Enhanced Carrier Route; Standard Mail regular flats and parcels; and Periodicals.[10] These services currently comprise 26 percent of USPS mail volume. Because these services also include mail that is not excepted by the PES, the proportion of mail-flow at risk of diversion would be between 0 and 26 percent.

The proportion would likely be considerably lower than 26 percent because (1) Standard Mail parcel prices may remain competitively low; (2) many parcels will not fit into a mailbox; (3) Express Mail requires a signature; (4) locked mailboxes, cluster-box units (CBUs),[11] and Post Office Boxes will likely remain monopolized by the USPS; and (5) private courier companies will likely continue to use the USPS's Parcel Select service for delivering parcels to areas in which it is very costly for them to make deliveries.

As in the experience of European countries, diversion may take some time to occur, but some diversion of mail to private couriers is a likely outcome. For example, in 2006, the UK's Postal Services Commission fully liberalized its postal services, opening them up to competition. In the two years since full liberalization, 19 companies have been licensed to provide postal services in the UK. Together, these companies have captured 20 percent of the total upstream market (collection, sorting, and transportation of mail) and 40 percent of the bulk mail sent by businesses. However, there has been almost no competition for providing full end-to-end service (collection to delivery), with approxi-

---

[10] The USPS predicts that the categories that would be most affected would be nonaddressed advertisements that saturate urban and suburban areas using Standard Mail Enhanced Carrier Route and Periodical services, delivered by low-cost local providers (Weaver, 2008).

[11] CBUs are typically stand-alone units that have multiple locked compartments for delivering mail to multiple recipients at a single address (such as an apartment building). Mail is typically delivered by opening the entire front or back panel of the unit. CBUs may also have compartments for outgoing mail or parcel lockers. Neighborhood delivery and collection-box units (NDCBUs) are similar to CBUs but serve multiple addresses (e.g., all homes on a cul-de-sac).

mately 99 percent of letters sent to addresses in the UK still being delivered by the Royal Mail (Hooper, Hutton, and Smith, 2008).

The Public Safety and Security Roles of the USPS and Private Couriers

National Response Framework and Cities Readiness Initiative

Both the USPS and private couriers play a role in public safety; however, the USPS's and IS's roles in public safety and homeland security are more formalized and extensive than those of private couriers. For example, under the National Response Framework (NRF), the USPS is designated as a supporting agency for seven of the 15 Emergency Support Function annexes (ESF). Under ESF-1 (Transportation), the USPS role is to report on infrastructure disruption and damages. Under ESF-8 (Public Health and Medical Services), the USPS is to assist in distributing and transporting medicine, pharmaceuticals, and medical information to members of the general public affected by a major disaster or emergency. As part of the response to Hurricane Katrina, the USPS provided mail services to relocated populations under ESF-6 (Mass Care, Emergency Assistance, Housing, and Human Services).

In addition, the USPS is currently involved in the Cities Readiness Initiative (CRI)—a pilot program involving 72 cities designed to help major cities and metropolitan areas increase their capacity to deliver antibiotics and other medical supplies to their populations within 48 hours in the event of a bioterrorism incident or other large-scale public health emergency (CDC, 2007). The USPS is working with seven CRI cities to develop a USPS antibiotic-delivery plan and is piloting the recruitment of volunteer mail carriers in Minneapolis–St. Paul, Minnesota. The delivery plan has been tested in three cities.[12] The plan concept is intended to reduce the potential surge at identified public health Points of Dispensing (PODs) in the event of a bioterrorism incident.

[12] Postal workers who volunteer to participate in the CRI will have antibiotics pre-positioned in their homes and regularly updated for themselves and their families.

In comparison, private couriers do not have a specified formal role in the NRF, although some couriers have been involved in the response to major disasters. For example, during Hurricane Katrina, FedEx helped move relief shipments, including equipment for the American Red Cross, in preparation for the storm (FedEx, undated[a]). At the request of the Centers for Disease Control and Prevention (CDC), UPS Air Cargo also helped transport pharmaceutical supplies and move equipment into the affected area. UPS Ground also assisted in moving relief supplies (UPS, undated[c]). In addition, the major couriers are involved with national associations, such as the Business Roundtable, that take on such issues as improving the security of U.S. critical infrastructure.

National Infrastructure Protection Plan

Both the USPS and private couriers participate in the National Infrastructure Protection Plan (NIPP), a U.S. Department of Homeland Security (DHS) initiative intended to provide a unifying structure for integrating existing and future critical infrastructure and key assets protection efforts (DHS, 2006). However, the degree of involvement varies. The NIPP calls for public-private security partnerships to share information and protect critical infrastructure and key assets. The USPS cochairs the Postal and Shipping Sector led by the Transportation Security Administration (TSA). Although courier companies also participate in the NIPP, indications are that the TSA is finding it challenging to get private companies on board, especially the smaller courier services.

Customs-Trade Partnership Against Terrorism

Like the USPS, the major private couriers also participate in the Customs-Trade Partnership Against Terrorism (C-TPAT), a volunteer supply chain–security program launched in 2001 and overseen by U.S. Customs and Border Protection (CBP) to improve security practices in light of terrorist threats. Participating companies are required to adhere to C-TPAT security criteria that address security training and awareness, container security, physical access controls, personnel security, procedural security, physical security, and information-technology

security (Skinner, Kelly, and Tenney, 2008). Air, rail, and sea carriers, importers, freight forwarders, and other import-logistics service companies are eligible to participate in the program. "Member companies agree to allow CBP to validate their security practices and, in exchange, they are awarded benefits, such as reduced scrutiny of their cargo" (GAO, 2008). For example, FedEx and DHL are C-TPAT–certified. Although CBP has taken steps to improve the security validation process, it still faces challenges in verifying that C-TPAT members' security practices meet minimum criteria. Further, there is wide variation in the participation rates among different-size couriers.

Carrier Alert

Arguably, at the local level, the USPS has more of a presence than do private couriers and a more central role to play in terms of neighborhood safety. For example, in 1982, the USPS, in collaboration with the National Association of Letter Carriers (NALC), established the Carrier Alert program. Through this program, letter carriers can detect whether any suspicious incidents or accumulation of mail occurs among customers who register for the program, allowing letter carriers to identify when customers may be unable to collect their mail because of illness, injury, or death (USPS, undated[a]). Although participation level in the Carrier Alert program has varied over time, the program is now being revitalized.

Public Safety Education and Awareness

In addition to the measures the USPS has implemented to safeguard the mail before it is deposited in a mailbox, the USPS and IS have also implemented public education outreach and awareness campaigns to educate the public about different types of mail crime, how customers can prevent themselves from becoming victims of such crimes, and what customers can do if they become victims of a mail crime. For example, following the 9/11 terrorist attacks, the USPS sent postcards to all residences and businesses in the nation with information on what to look for in suspicious mail and packages (USPS, 2001d). In 2008, the USPS sent out millions of postcards, including about 100,000 in Maine, warning people about soda bottles filled with volatile chemicals

that had been left in mailboxes in the state (Russell, 2008). The USPS has also undertaken a number of public safety education campaigns, such as on public awareness of fraud and identity theft, using dollars collected from fines to support those campaigns. Table 2.1 provides an

Table 2.1
USPS Guidance and Training to Private Businesses and the Public

Title	Description
Guidelines	
"It's What's Inside and How It's Packed"	This poster provides visual and written descriptions of what is allowed and not allowed to be sent through the mail and instructions on how to package certain mailable items that may be mistaken as suspicious or hazardous (USPS, 2007).
"Suspicious Mail or Packages"	This poster presents the guidance in a poster for USPS and private mail-room employees (USPS, 2006f). For further description of the three Ps, see Table C.1 in Appendix C.
"Keep the Mail Safe"	This poster provides a detailed table of hazardous materials that may and may not be sent through the mail, with graphics and examples of different types of hazardous materials (USPS, 2006d).
"Notice of Reward"	This poster lists each type of offense for which the IS offers a reward and provides the name and description of the offense and the monetary amount of the reward.
"Best Practices for Mail Center Security: Incoming and Outgoing Operations"	This guide provides general advice to mail-center supervisors and their coworkers and recommends protective measures to help assess, prevent, and respond to three types of threats: mail theft, package bomb or bomb threat, and chemical, biological, or radiological threats (IS, undated).
"Don't Let One Phone Call Take It All Away"	This poster provides contact information for elderly consumers who are victims of financial fraud and have lost money as a result (IS, 2001).
"Look Before You Cash!"	This brochure describes what genuine U.S. Postal Money Orders look like and provides guidance on what features to look for before accepting or cashing one (USPS, 2005c). It is intended to prevent money order fraud.
"Hang Up on Phone Fraud"	This brochure briefly describes the threat of telemarketing fraud and how consumers can protect themselves against it (IS, 2004b).

Table 2.1—Continued

Title	Description
"Safeguard Your Personal Information"	This booklet provides an overview of what identity theft is, tips for consumers to protect themselves from it, and what a victim of identity theft can do. It also describes how consumers can keep their personal information safe from online prowlers (IS, 2007e).
"Consumer Fraud by Phone or Mail: Know How to Protect Yourself"	This brochure provides an overview of the types of consumer fraud that can occur over the phone or via the mail and describes the typical pitch used. It provides guidance on what consumers can do and who to contact if victimized (IS, 2006c).
"A Consumer's Guide to Sweepstakes and Lotteries"	This booklet provides consumers with guidance for responding to sweepstakes offers and for recognizing the difference between legitimate sweepstakes and other types of offers (such as prize promotions) and other illegitimate promotions that misrepresent themselves and seek to defraud (IS, 2007d).
"Ensuring the Security of Apartment Mailboxes"	This brochure provides guidance that old apartment mailboxes should be replaced with newer, more-secure unit mailboxes. It also provides guidance on the type of unit mailboxes that are most secure and provides contact information for mailbox distributors.
"Don't Be the Victim of a Check Scam!"	This brochure provides a brief overview for consumers describing check scams, how to avoid being a victim of one, the consequences of being involved in one, and whom victims should contact (IS, 2008b).
"U.S. Postal Inspection Service Guide to Preventing Mail Fraud"	This booklet provides consumers and businesses with guidance on how to identify different types of mail fraud. The booklet describes many different types of mail fraud and describes how to contact the IS (IS, 2007c).
A Law Enforcement Guide to the U.S. Postal Inspection Service	This guide helps federal, state, and local law enforcement agencies understand the IS's authority, capabilities, and the crimes that the IS investigates. It provides information on postal crimes for which a U.S. Postal Inspector should be notified. It also provides an overview of how the IS can assist other law enforcement agencies (IS, 2006d).
Training videos	
Truth or Consequences: Fake Check Scams	This video discusses fake-check scams (IS, 2004g).
All the King's Men: Picking Up the Pieces	This video discusses fraud schemes that victimize millions of Americans each year, leaving many financially devastated, and urges victims to learn more about their rights (IS, 2006a).

Table 2.1—Continued

Title	Description
Nowhere to Run: Cross-Border Fraud	This video illustrates how U.S. Postal Inspectors created task forces with Canadian law enforcement partners to stop cross-border scams (IS, 2005a).
Web of Deceit: Internet Fraud	This video tells the story of a scammer who uses the Internet to victimize unsuspecting consumers around the world until he gets caught in his own web of deceit and provides tips on what to watch out for when doing business on the Internet (IS, 2005b).
Long Shot: Foreign Lottery Scams	This video tells the story of a foreign-lottery fraud victim and the con artist behind the scam and provides tips on avoiding becoming a victim of this scam (IS, 2004d).
Work-at-Home Scams: They Just Don't Pay	This video tells the story of a new type of work-at-home scam and how a young mother gets caught up in it. It provides tips on how to avoid being duped by criminals and what to do if victimized by a work-at-home scam (IS, 2004e).
Identity Crisis: Protect Your Identity	This video tells the story of a couple whose credit is ruined and of the criminals who defrauded them. It provides tips on how to protect against identity fraud and what to do if victimized (IS, 2004c).
Dialing for Dollars: Telemarketing Fraud	This video tells the story of a scam and the lives that have been ruined by it. It provides tips on how to protect against investment fraud and what to do if victimized (IS, 2004a).

overview of the different types of public awareness and outreach efforts the USPS and IS currently conduct. Appendix C provides a detailed list of USPS employee guidance and training.

The USPS also currently provides training to non-USPS entities. For example, it provides training to private businesses' mail-room operators on how to detect and respond to suspicious- or hazardous-mail incidents. For example, in 2007, the IS partnered with the Postal Customer Council to develop seminars for mail-center managers to help them establish such practices for handling their mail operations. In addition, the USPS provides security training to other federal, state, and local agencies.

The Role of the IS in Public Safety and Security

The IS is one of the nation's oldest federal law enforcement agencies. It exists pursuant to Congress's power "to make all Laws which shall be necessary and proper" to perform the obligation provided by the U.S. Constitution "to establish Post Offices and post Roads" (Art. I, § 8, cl. 7). The role of the IS is to safeguard the nation's mail, to protect the integrity of the postal system, and to ensure that the postal system is not used for illegal purposes (President's Commission on the United States Postal Service, 2003, p. 99). As the President's Commission on the United States Postal Service noted,

> The Postal Inspection Service enforces more than 200 Federal laws, ranging in purpose from protecting employees against workplace violence to cracking down on drug trafficking to exposing workers' compensation fraud to tracking down the culprits who steal people's mail. In addition, the [IS] has a number of investigatory responsibilities. . . . [It is] responsible for looking into possibly fraudulent activity relating to mailings, postage, and meters; fraud against consumers, business, and government; crime prevention and security; mail theft; prohibited mailings (child exploitation, bombs and drugs); robberies and burglaries; assaults and threats; [and] money orders, financial instruments, and postal property crimes. (President's Commission on the United States Postal Service, 2003, pp. 99–100)

The IS employs nearly 3,000 professionals: 1,689 Postal Inspectors, 735 Postal Police Officers, and 564 technical and administrative support staff (USPS, 2007; OIG, 2008).

Postal Inspectors trained as dangerous-mail investigations (DMI) specialists routinely screen packages and mail (including screening packages coming through private couriers) for explosives or other dangerous materials for such venues as the Republican National Convention, the Democratic National Convention, the Super Bowl, the Olympic Games, and other major sporting events (IS, 2008a).

Before 9/11, Postal Inspectors participated to varying degrees with the Federal Bureau of Investigation's (FBI's) regional Joint Ter-

rorism Task Forces (JTTFs), providing information and assisting with investigations; however, this participation grew substantially following the attacks. Since 9/11, the IS has had a full-time liaison at the FBI's National JTTF. Also, the IS has a full-time liaison at DHS's National Operations Center (IS, 2008a).

The IS also collaborates with federal, state, and local law enforcement agencies on a number of interagency task forces. For instance, it participates in two of the four working groups on the President's Identity Theft Task Force and leads or co-leads a number of financial crime task forces and working groups (IS, 2008b, p. 20). According to the IS, "Postal Inspectors conduct more identity theft investigations than any other federal law enforcement agency in America" (IS, 2008b, p. 20). It also collaborates with local law enforcement agencies and district attorneys to investigate crimes that are not of broad enough scope to be accepted for prosecution by the local U.S. Attorneys Office.

In addition, the IS investigates child-exploitation crimes, successfully rescuing 52 children from sexual abuse in 2007 and 93 in 2006 (IS, 2008a, p. 2; IS, 2007a, p. 2).

Internationally, the IS works to intercept counterfeit documents before they get into the mail stream abroad en route to the United States. Nigerian fraud letters are one example, with these letters often being routed through Canada. Between January and August 2007, the IS's Global Counterfeit Initiative seized 540,000 counterfeit checks and Postal Money Orders valued at more than $2.1 billion from the mail (IS, 2008a, p. 2). As a member of Operation Global Con, the IS contributed to 45 of 96 investigations that identified 2.4 million victims who suffered losses of $1 billion from mass-marketing fraud schemes (IS, 2007a, p. 2).

CHAPTER THREE

Relaxing the Mailbox Rule: Effect on Public Safety and Security Incidents

As of 2007, the USPS was responsible for processing and delivering 213 billion pieces of mail per year, or roughly 700 million pieces of mail per day, to more than 148 million homes, businesses, and Post Office Boxes throughout the United States (USPS, 2008). Given the sheer magnitude of mail for which the USPS is responsible daily and that one of its primary concerns is to protect the mail, its employees, and the public, the USPS and the IS use a myriad of training courses, formal guidance, and policies and procedures to promote the safety and security of the mail throughout the postal system.

In this chapter, to the extent possible given the data limitations described above, we assess possible public safety and security implications of relaxing the Mailbox Rule, with a focus on the potential impact on the numbers and types of reported security incidents. We start by analyzing the IS incident data set for 2004 through 2007,[1] with an eye toward understanding the types of security incidents that occurred and the trends over time for those incidents with the monopolies in place. If the Mailbox Rule were to be relaxed, the role of private courier services in delivering mail will likely increase, as will their access to the mailbox; thus, we next examine two key issues—differences between the USPS and private couriers in training, accountability, and oversight—that may affect public security and safety. Finally, we discuss what we believe might be the general implications of relaxing the Mailbox Rule and the specific implications for different types of security incidents.

[1] When the data are available, we also analyze 2003 incidents.

Types of Security Incidents and Trends

To what does *public safety and security* refer when we consider different types of incidents? It means physical safety from dangerous items that the USPS does not allow to be mailed or regulates heavily, such as hazardous materials (chemical, biological, or radiological) and bombs and other explosive devices. It also means protection from a wide array of fraud, such as identity theft, credit card theft, check fraud, and employment and investment schemes. In addition, it means the security of the mail itself—from mail theft, from volume attacks (e.g., mail theft from apartment panels or CBUs), and from attacks on mailboxes themselves.

To assess the number of security incidents in the mail, the primary sources of data are the IS's three databases that provide information related to public safety and security: its Fraud Complaint System (FCS), its Financial Crime Database (FCD), and its Suspicious Incident Reporting System (SIRS). Volume attacks represent a subset of the FCD, and bombs/improvised explosive devices (IEDs) represent a subset of the SIRS. We analyze these types of incidents separately using the following five categories:

1. *volume attacks*, a special subset of the FCD involving instances in which mail is stolen from a multiple-mailbox location (such as apartment panels)
2. *fraud data*, incidents in which the IS is contacted about questionable or fraudulent activity involving the mail
3. *financial crimes*, finance-related crimes that have been perpetrated through, or aided by, the postal system. This database consists of incidents in which the IS was contacted about finance-related crimes, typically by financial institutions, credit-card companies, retailers, or consumers.
4. *suspicious incidents*, instances in which there is some problem with a piece of mail and a Postal Inspector visits a site to investigate the contents. USPS employees initiate the majority of these incidents, but there are also incidents originating from customers when they receive an item. Virtually all the suspicious incidents

in the years covered were false alarms; however, many of the incidents involved written or spoken threats, including threats that an item may contain some type of hazardous materials.

5. *IEDs (bombs)*, a special subset of SIRS involving actual explosives and perceived or explicit threats, which, for our purposes here, we address as a distinct group.

In addition to using the IS databases, we incorporate information from the U.S. Census Bureau into our analysis to estimate whether each reported incident occurred in a rural or urban ZIP Code setting,[2] as well as to estimate the occurrence of reported incidents by median household income within the ZIP Code.[3]

There are several limitations to these data. It is important to note that these databases include only detected and reported incidents, so they cannot be assumed to reflect *all* incidents. The fraud and financial crime data are limited to the subset of crimes involving the postal system and are dependent, at least in part, on outside persons knowing to report the incidents to the USPS. Some types of incidents may be more likely to be reported to the USPS than others are, regardless of the actual number of incidents that occur. Hence, the true level of fraud and financial crime occurring, even that involving the postal system, cannot be obtained from these data. Similarly, the vast majority of the suspicious-incident reports ultimately did not involve potential harm to the public. It should be noted that government agencies are highly incentivized to be exceedingly cautious (particularly post-9/11) to avoid

---

[2] The Census Bureau defines an *urbanized area* as consisting of a central city and surrounding areas with a population greater than 50,000. In addition, other towns outside of an urbanized area whose populations exceed 2,500 are included in the urban population, leaving all other areas rural. According to this definition, the 2000 census indicates that 21 percent of the population lived in rural areas. Because ZIP Codes do not fit standard census measures of geographic space and may overlap both Census Bureau–defined urban and rural areas, we treat ZIP Codes in which 50 percent or more of the 2000 population lived in rural areas as *rural*.

[3] We define *low-income* ZIP Codes as those ZIP Codes with a median household income level at or below the 30th percentile based on projected 2008 income levels from the 2000 census (GeoLytics, 2006). *High-income* ZIP Codes are defined as ZIP Codes with median household incomes at or above the 70th percentile.

possibly catastrophic outcomes of overlooking a hazardous item. However, many of these "safe" incidents include threats or hoaxes (which are crimes in themselves), which are identified separately in the analyses. Additional caveats about the data contained in the IS databases are discussed in Appendixes A and D.

Despite the limitations associated with these data, they are capable of providing a valuable description of many of the types of crime and safety issues associated with the mail, as well as providing a useful baseline level for each type of mail-related crime on which to base projections.

In this section, we first present descriptive summaries of each type of incident, including trends over time, how they vary by potential to do physical or financial harm to USPS customers, where they are most likely to be detected along the processing and delivery channel, and how these incidents vary by urban and rural areas and by higher- and lower-income neighborhoods. The descriptive summaries provide a baseline level for subsequent projections of how such security incidents may change in light of differences between USPS and private couriers in training, accountability, and oversight (discussed immediately afterward). Appendix B provides detailed tabular displays from our analysis of the IS incident databases.

Volume Attacks

Volume attacks are instances in which mail is stolen from a multiple-mailbox location. In 2007, there were nearly 6,000 volume attacks. Table 3.1 shows the percentage of volume attacks by year from 2004 to 2007. Neighborhood delivery and collection-box units (NDCBUs) were the most targeted receptacles (57 percent of attacks), followed by apartment panels (20 percent) and CBUs[4] (12 percent). Figure 3.1 is a photograph of a typical CBU.

[4] CBUs are typically stand-alone units that have multiple locked compartments for delivering mail to multiple recipients at a single address (such as an apartment building). CBUs may also have compartments for outgoing mail or parcel lockers. NDCBUs are similar to CBUs but serve multiple addresses (e.g., all homes on a cul-de-sac).

Table 3.1
Volume Attacks, by Year

	Year (%)			
Receptacle Type Attacked	**2004**	**2005**	**2006**	**2007**
CBU	10.0	10.2	13.1	12.1
NDCBU	50.7	56.1	61.4	56.9
Post Office Box (5+)	1.7	1.3	1.2	2.9
Apartment panel	25.1	22.2	17.1	19.5
Carrier robbery	3.2	1.6	1.8	1.0
Other	9.3	8.6	5.4	7.6
Total number of incidents	8,767	9,415	6,375	5,952

Figure 3.1
Cluster-Box Units, One Type of Multiple-Mailbox Delivery Point

SOURCE: Copyright Design Pics.
RAND *MG800-3.1*

Between 2004 and 2007, the number of volume attacks declined by 32 percent (from 8,767 to 5,952).[5] As shown in Table 3.2, which breaks down volume attacks by sociodemographic context, most volume attacks occur in urban areas (90 percent); however, the type of receptacle attacked varies between urban and rural areas. For example, in urban areas, NDCBUs (52.7 percent) and apartment panels (24.0 percent) are the most common targets of volume attacks. In rural areas, NDCBUs are the most common targets (76.6 percent), with only 4.9 percent of apartment panels being identified as targets.

The type of receptacle that is targeted also varies by neighborhood income, which is also shown in Table 3.2. Volume attacks are substantially more prevalent in higher-income neighborhoods than in lower-income neighborhoods: Of all volume attacks, 68.3 percent were in higher-income ZIP Codes, compared with only 1.7 percent in lower-

Table 3.2
Volume Attacks, by Sociodemographic Context

Receptacle Type Attacked	% of All Urban Neighborhood Attacks	% of All Rural Neighborhood Attacks	% of All Low-Income Attacks	% of All High-Income Attacks
Apartment panel	24.0	4.9	11.1	23.7
Carrier (robbery)	2.3	0.0	18.1	0.8
CBU	11.3	11.1	1.5	13.1
NDCBU	52.7	76.6	16.8	56.2
Post Office Box (5+)	1.2	3.9	25.3	0.8
USPS vehicle	4.0	0.0	15.7	2.2
Percentage of all volume attacks	90.0	10.0	1.7	68.3

NOTE: Income columns do not total 100 percent because they account for only low- and high-income neighborhoods.

[5] This does not appear to be an artifact of the data-collection or -entry processes—that is, the decline in reported incidents appears to be real and does not reflect delays between the event and the entry of an incident into the database.

income ZIP Codes. In lower-income neighborhoods, a disproportionately high number of attacks occur on Post Office Boxes, USPS vehicles, or USPS carriers themselves. In higher-income neighborhoods, more attacks occur on CBUs, apartment panels, and NDCBUs.

Fraud

As mentioned, the IS collects fraud data when it is contacted about questionable or fraudulent activity involving the mail. The types of fraud schemes that the IS monitors are summarized in Table 3.3.

Table 3.3
Types of Fraud Schemes

Type of Fraud Scheme	Description
Advance payment	Inducement to pay fees for services promised at a future date
Chain letter	Mailings that promise recipients something of value if they keep the chain unbroken and remit money
Charity fraud	A solicitation purporting to be for a worthy cause that is, in fact, for private gain
Education	An offer that involves a fraudulent educational opportunity, promising either enrollment in a school or the attainment of a degree for a fee or other investment
Employment	Misrepresentation of employment opportunities, offering nonexistent employment or providing false or obsolete employment-test materials or information for a fee
False bill or notice	An invoice or bill for a product or service never ordered or provided
Harassment	A typically unknown source of complaint orders merchandise or sends offensive materials in the victim's name without his or her consent (e.g., obscene literature, products)
Investment	Promises of extraordinary financial returns following an initial investment; in some instances, victims experience a small return, thus enticing them to make larger financial contributions, but large returns never materialize
Lottery	Advertisements seeking money or property by mail for participation in schemes to win prizes through others' efforts over which the participant has no control

Table 3.3—Continued

Type of Fraud Scheme	Description
Medical quackery	Promises exaggerated and unfounded cures through worthless medical products
Merchandise or service (other than travel, personal service, or other named categories)	Obtains money or property for inferior, misrepresented, or undelivered goods or services
Nigerian fraud	A swindle boasting a unique business opportunity to earn a lot of money through a Nigerian official; such mailings often have specific characteristics for which the USPS looks
Personals	Extracts money in exchange for undelivered or misrepresented personal services, such as dating services, mail-order partners, or false divorce decrees
Prize or sweepstakes	Requires advance payment or fee to receive a "free" prize or to enroll in a nonexistent sweepstakes; prizes either are never shipped or are inferior to what was promised
Sexually oriented advertising	Graphically depicts or explicitly describes, in a predominantly sexual context, human genitalia or any sexual act
Underpaid postage	Offers to provide information on how to send first-class mail with less than the proper postage amount
Vacation or travel	Offers vacation, time-sharing, or travel opportunities that are misrepresented, not delivered, or delivered with hidden fees

There were more than 32,000 reports of fraud in 2007 (Table 3.4). The most common types of reported fraud were merchandise or services (45.6 percent), Nigerian fraud (11.7 percent), false bills or notices (11.2 percent), and prize or sweepstakes (9.6 percent).

Between 2003 and 2007, the total number of fraud reports declined to 66 percent of the 2003 level (from 49,258 to 32,353). The decline occurs across the different categories of fraud, with two exceptions: Nigerian fraud (rose from near 0 percent in 2003 to 12 percent in 2007) and false bill or notice (rose from 7 percent in 2003 to 11 percent in 2007). In approximately half (55 percent) of reported fraud cases, victims were initially contacted through the U.S. mail.

Table 3.4
Reported Fraud Incidents, by Year

	Year (%)				
Type of Fraud	**2003**	**2004**	**2005**	**2006**	**2007**
Employment	5.0	4.6	3.6	3.4	3.3
False bill or notice	7.4	9.0	6.9	9.0	11.2
Lottery	9.1	10.1	16.3	4.6	6.2
Merchandise or service	58.0	51.0	36.7	50.5	45.6
Nigerian fraud	0.2	0.4	2.1	8.5	11.7
Prize or sweepstakes	11.5	13.7	24.4	13.6	9.6
Other	8.8	11.2	10.0	10.4	12.4
Total number of fraud incidents	49,258	44,142	49,352	30,516	32,353

A higher percentage of urban-area reported fraud consisted of merchandise or service and false bill or notice, while rural areas had more reports of lottery and prize or sweepstakes fraud (Table 3.5). These types of fraud also varied by neighborhood income level. Higher-income neighborhoods were more likely to report fraud related to merchandise or service and lottery, while lower-income areas were more likely to report fraud related to false bill or notice and prize or sweepstakes schemes.

The impact of fraud on the consumer varies. Overall, the median reported loss from fraud was $116. However, there was a wide range in the amount of reported loss:[6]

- $2,601 for Nigerian fraud schemes

[6] The median value for each fraud category is reported because it is less sensitive to extreme values than are other measures. Information on the amount of financial loss resulting from each of the reported fraud incidents is available in roughly half of all cases. While this suggests that only half of the reported fraud attempts successfully led to victimization, it is also possible that loss values were not reported for some successful fraud attempts and that some reported losses actually reflect the "promised" return rather than money initially lost (e.g., reporting "loss value" as the grand prize in a sweepstakes rather than money actually spent to participate in the sweepstakes). Thus, the loss values should be interpreted with caution.

Table 3.5
Reported Fraud Incidents, by Sociodemographic Context

Type of Fraud	% of All Urban Neighborhood Attacks	% of All Rural Neighborhood Attacks	% of All Low-Income Attacks	% of All High-Income Attacks
Advance payment	2.6	2.5	3.7	2.2
False bill or notice	9.0	7.4	10.8	9.4
Lottery	9.4	10.8	6.4	9.6
Merchandise or service	47.0	44.7	45.7	48.6
Nigerian fraud	5.2	6.1	4.9	5.0
Prize or sweepstakes	14.8	17.4	14.9	13.5
Other	3.2	11.1	13.6	11.7
Percentage of all reported fraud incidents	84.2	15.8	5.0	60.4

NOTE: Income columns do not total 100 percent because they account for only low- and high-income neighborhoods.

- $1,400 for investment schemes
- $598 for vacation and travel schemes
- $300 for advance-payment schemes
- $112 for merchandise and service schemes
- $80 for false bill or notice schemes
- $59 for employment schemes.

An estimated 6.6 percent of fraud reports resulted in opening a criminal case or arrest; generally, the IS appears to pursue a case or arrest for the most prevalent types of fraud.

Financial Crime

There are many types of financial crime. Table 3.6 itemizes key examples of the different types of financial crime on which the IS collects

Table 3.6
Selected Types of Financial Crime

Type of Financial Crime	Description
Check fraud (lost or stolen)	Delinquency of receipt or theft of financial checks sent though the mail
Credit card	Credit card not received or stolen from the mail
Fraudulent application (financial)	Fraudulently obtaining a credit or debit card by falsifying information provided to a credit issuer on an application using the mail to obtain or transfer information or services
Identity theft	Use of another person's identifying information to fraudulently establish credit, take over a victim's financial accounts, obtain loans, rent apartments, or obtain services with utility companies using or through the postal system
Mail tampering	Mail received open with contents
Mail theft (mail not received)	Incoming or outgoing mail stolen
Mail theft (mail received open)	Mail received without contents

information. A full description of the types of financial crime tracked is given in Table B.3 in Appendix B.

As shown in Table 3.7, there were more than 5.2 million reports to the IS of financial crimes committed through the U.S. postal system in 2006 and 2007 (the years reported here).[7] Each reported incident may include one or more of the classifications listed in Table 3.6, and, thus, values may sum to more than 100 percent. The overwhelming majority of reported financial crimes involve mail theft, in which the mail has not been received (96.8 percent). In addition, 28.8 percent of reported financial crime incidents involve theft of credit cards, and 57.7 percent of reported financial crime incidents included mail theft involving audio or visual items, such as rental DVDs or computer games. Although lost- or stolen-check fraud and identity theft represented

[7] The 2006–2007 data were the only data made available for this study. The IS purges historical data periodically because of data space constraints, of which the financial crime data represent the greatest concern. Because no meaningful trend in crimes from 2006 to 2007 could be identified, the data were pooled.

Table 3.7
Reported Financial Crime Incidents for 2006–2007

Type of Crime	Percentage of Total Crimes Involved
Check fraud (lost or stolen)	3.57
Credit card	28.83
Fraudulent application (financial)	1.13
Identity theft	1.01
Mail tampering	1.03
Mail theft (mail not received)	96.82
Mail theft (mail received open)	0.49

NOTE: The total number of financial crime incidents was 5,240,605.

only 3.6 percent and 1 percent of reported incidents, respectively, these crimes may be more frequently reported to other entities (such as financial institutions, state or federal consumer organizations, or other law enforcement agencies) even if the incident involves the mail.

Most of the reported financial crimes involving the mail occurred in urban areas (90 percent) (Table 3.8). Rural areas reported disproportionately more credit card theft. This may reflect differences in reporting of credit card theft between urban and rural areas to the IS versus local law enforcement, for example. Consumers in urban areas reported to the IS proportionately more identity theft and fraudulent financial applications than those in rural areas.

Higher-income neighborhoods were more linked to reports of identity and mail theft, while reports of check fraud, credit card theft, and fraudulent financial applications were more associated with lower-income neighborhoods.

We also examined the type of receptacle in which the mail was originally deposited, by rural or urban ZIP Code (not shown; see Table B.10 in Appendix B). In the vast majority of reported financial crime incidents (98.0 percent), the receptacle was not recorded. However, when the receptacle was recorded, rural boxes were the most commonly identified type of receptacle (32.5 percent), followed by

Table 3.8
Reported Financial Crimes, by Sociodemographic Context for 2006–2007

Type of Crime	% of All Urban Neighborhood Attacks	% of All Rural Neighborhood Attacks	% of All Low-Income Attacks	% of All High-Income Attacks
Check fraud (lost or stolen)	3.67	3.66	3.7	2.2
Credit card	24.85	28.98	10.8	9.4
Identity theft	1.08	0.97	6.4	9.6
Mail theft (mail not received)	97.34	97.29	45.7	48.6
Fraudulent application (financial)	0.54	0.47	14.9	13.5
Percentage of all reported financial crime incidents	89.8	10.2	26.7	40.5

NOTE: Income columns do not total 100 percent because they account for only low- and high-income neighborhoods.

apartment panels (18.6 percent), porches (14.2 percent), and CBUs (12.1 percent). The crimes most often associated with incidents that contained receptacle reports were mail theft with mail not received (60.4 percent), mail tampering (15 percent), and mail received open (6.6 percent).

Identity theft and theft of credit cards, as well as other types of mail theft, are a growing concern in other countries as well. For example, to address this concern, Canada Post is currently in the process of upgrading the locks on its "street furniture" to reduce the risk of mail theft. Its crown locks and keys are unique to Canada Post, with it being a criminal offense to be in possession of such keys or any container used to store mail without a lawful reason.[8] In Canada, mail delivered to an apartment building is usually delivered to a lockbox assembly (panel of

[8] Canada Post has a de facto mailbox monopoly for letters mailed to locked mailboxes; only Canada Post has access to locked community mail boxes, group mailboxes, or post office lockboxes.

locked compartments) with access limited to Canada Post. In addition, new residential developments have community mailbox delivery (central locked set of boxes) to which only Canada Post has access.

Suspicious Incidents

The USPS classifies suspicious incidents into the following categories:

- leaking gas, liquid, or powder
- radiological alerts
- suspicious mail with no substance found
- suspicious substance inside (or outside) a USPS facility
- mail that involved a written or spoken physical threat (with or without a substance)
- other unspecified incident.

In Table 3.9, we show the most common types of suspicious incidents reported between 2003 and 2007. Also, note that the suspicious incidents examined in this subsection exclude IEDs (bombs), which are discussed in the next section. Recall that, in almost all cases, the reported suspicious incidents were ultimately not to present a real security or health hazard. While leaking substances may have the potential to damage other mail, upon inspection, the leaking substances were rarely found to be dangerous. Similarly, radiological alerts identified radioactive substances, but the substances were not actually dangerous

Table 3.9
Suspicious Incidents, by Year

	Year (%)				
Type of Incident	**2003**	**2004**	**2005**	**2006**	**2007**
Leaking gas	0.4	0.6	1.5	2.4	1.8
Leaking liquid	4.6	4.4	8.9	11.0	16.6
Leaking powder	56.7	64.1	68.6	76.6	71.4
Other	38.3	30.9	21.0	10.0	10.2
Total number of suspicious incidents	1,124	1,466	1,912	2,649	3,016

items. Mail with accompanying explicit threats do inherently involve public safety concerns, but they were virtually all hoaxes or did not include actually hazardous materials during the time period covered here. Further, reports of suspicious incidents involving explicit threats declined substantially from 2003 to 2007, from more than 18 percent to less than 1 percent of incidents (see Table B.11 in Appendix B).

More than 3,000 suspicious incidents were reported in 2007, most of which involved leaking powders (71.4 percent) or leaking liquids (16.6 percent).

The majority of suspicious incidents were reported at a USPS facility of some type (77 percent), with an additional 1.4 percent identified at a USPS collection box and 0.6 percent identified on a USPS vehicle. Most of the suspicious incidents were identified before delivery; only 21 percent of suspicious items were identified after delivery.

Over time, the number of reported suspicious incidents has increased steadily—at this writing, nearly triple the number reported in 2003 (from 1,124 to 3,016). This may reflect a true increase in the number of suspicious items, or it may reflect increased detection capacity (such as the introduction of radiological alert capacity in 2005) and more reporting of suspicious items. As discussed further later, it may be associated with changes in training, given the fact that training on identifying and reporting suspicious-mail incidents became mandatory for all USPS personnel beginning in 2003. Between 2003 and 2007, there were two fatalities and six injuries associated with suspicious items. This would argue that most suspicious items do not result in serious incidents. An exception is the case of anthrax. Given the USPS's experience in 2001 and 2002, in which the mailing of anthrax spores resulted in five deaths, 22 cases of anthrax, and the contamination of 23 USPS facilities (GAO, 2004a), one could argue that white-powder incidents potentially pose a serious threat. Although there have been many false positives detected since 2003, there could be catastrophic results if another real anthrax incident occurred.

The data suggest that the USPS appears to be identifying suspicious items more quickly in the processing and distribution cycle over time: The proportion of suspicious items identified *after delivery* declined from 2003 to 2007. For example, the number of suspicious

items identified after delivery to companies or firms declined from 9.4 percent in 2003 to 3.7 percent in 2007 and to residential locations from 8.4 percent in 2003 to 5.4 percent in 2007. During this same period, identification of suspicious items has increased at Processing and Distribution Centers (P&DCs) (from 15.9 percent in 2003 to 21.9 percent in 2007) and at international service centers (Airmail) (from 0.5 percent to 5.6 percent). These trends could be related to the fact (stated earlier) that training on detection of suspicious items became mandatory at the national level in 2003.

In addition, the IS appears to be taking more control over responding to suspicious items. In 2007, 81 percent of all incidents were handled exclusively by the IS, without involvement from other agencies (Table 3.10). This percentage has increased from 2003, when only 65 percent of such incidents were handled exclusively by the IS. Similarly, the IS has increasingly become the first responder to reports of suspicious items, rising from 65 percent of cases in 2003 to 91 percent in 2007.

Letters and small packages appear to be the more common mode of delivering suspicious material. Overall, 39 percent of all reported suspicious items were originally sent via First-Class Mail, suggesting that these were primarily letters, large envelopes, or small packages. Two percent of suspicious items were sent by Parcel Post, suggesting that these were likely packages. Fifteen percent were sent by Priority

Table 3.10
Percentage of Incidents in Which the IS Was Involved

Year	Percentage of Incidents in Which the IS Was the Sole Agency Involved	Percentage of Incidents in Which the IS Was the First Responder
2003	65.4	65.3
2004	60.8	60.8
2005	64.8	83.4
2006	74.2	97.4
2007	80.6	91.1

Mail[9] or Express Mail, which could have been either letters or packages.[10]

Identification of suspicious items appears to occur later in rural areas; they were disproportionately more likely to have been identified after delivery.

As mentioned previously, we were not able to obtain data from private courier services to mirror the IS reported-incident data; in the absence of such data, this study may implicitly underestimate the courier services' ability to detect hazardous items or respond to public safety and security issues. However, the IS data do contain a small amount of information that offers an avenue into comparing the USPS and courier services, at least with regard to detecting suspicious items. Perhaps the most important information from the suspicious-item database for this study is that the USPS appears to have more-sensitive capabilities to detect suspicious items than do non-USPS carriers—a conclusion based on higher rates of predelivery identification among last mile items. These last mile items originated (undetected) from other carrier services and entered the USPS system en route to delivery. The USPS identified suspicious items in slightly more deliveries originating from non-USPS carrier services (but that entered the USPS system at some point) slightly more often (86.9 percent versus 78.7 percent of the time) than those handled exclusively by the USPS.[11] None of these last mile items had been identified as suspicious while in the non-USPS delivery channel. This may suggest that the level of detecting suspicious items is lower in the non-USPS channels; when items enter the USPS system from a courier or other non-USPS service, they appear to be

[9] Large or thick envelopes, tubes, and packages containing mailable items can be sent using Priority Mail; letters, large or thick envelopes, tubes, and packages containing mailable items can be sent using Express Mail (USPS, 2002b).

[10] For 28 percent of incidents, there was no information on mode of delivery.

[11] The IS data contain 267 items that originated from non-USPS services during this period. The distributions of types of suspicious incidents being identified are roughly similar between USPS and non-USPS items, with powders accounting for more than half of the incidents. However, the non-USPS items had a substantially higher radiological alert rate (14 percent versus 4 percent). It is not possible to compare whether these items are mostly letters or mostly packages in either case.

more readily and more quickly identified. By extension, this may also suggest that the USPS might have identified items as suspicious that were handled and delivered exclusively by non-USPS channels—that is, upstream in the distribution chain, the USPS might have detected the suspicious package, while other couriers may be more likely to pass them through the distribution chain without identifying potentially hazardous items. This finding suggests that the USPS does a better job of detecting suspicious items than non-USPS services. However, it is also important to keep in mind that virtually all the reports of suspicious incidents were false alarms.

Improvised Explosive Devices (Bombs)

In 2007, nearly 1,500 additional suspicious-incident reports were classified as being possible IEDs (Table 3.11). While more than 80 percent of these incidents did not actually involve explosives, legitimate IEDs represented 14 percent of the reported incidents and posed a real threat to the public.

Most reported IED or explosives-related suspicious incidents (92 percent) occurred in urban settings. While the total number of explosives-related suspicious incidents increased by 45 percent between 2003 and 2007, this primarily reflects a general increase in the number of false positives; the number of actual IEDs has not followed any particular trend over time (although, as a proportion of all types of suspicious explosives incidents, it has declined).

The most commonly reported way in which IEDs and other explosives-related suspicious items are distributed is through the USPS.

Table 3.11
IEDs, by Year

	Year (%)				
Type of Explosives Incident	**2003**	**2004**	**2005**	**2006**	**2007**
Actual IED	23.4	20.3	17.8	21.0	14.0
Other	76.6	79.7	82.2	79.0	86.0
Total number of explosives incidents	1,032	1,002	935	1,203	1,495

Approximately 31 percent both of all explosives-related suspicious items and of actual IEDs were mailed. The next most common method of distributing IEDs and other explosives-related items is in person or by hand[12] (approximately 25 percent). The remainder of suspicious incidents recorded the method of distribution as "unknown" (32 percent), "not applicable" (10 percent), or "verbal or written threat" (2 percent).

Although the data do not generally include the specific location where the IED or other explosives-related suspicious item was detected, one can infer that most of these items involve Post Offices and USPS facilities, because 30 percent of the items are being sent through the USPS. It also appears that at least 62 percent of the bomb-related suspicious incidents are detected at some sort of postal facility.[13] Specifically among actual IEDs, however, 75 percent of locations are not listed and cannot be determined from the data provided.

Differences Between the USPS and Private Courier Companies in Training, Public Accountability, and Oversight

The preceding section provided an overview of the types of crimes and security incidents connected to the mail that have occurred in recent years with the Mailbox Rule in place. It also pointed to some trends in reported incidents and in the USPS's response to those trends. This section examines two issues that are relevant to public safety and security, particularly in light of the diversion of mail to private couriers that would likely occur if the Mailbox Rule were to be relaxed: differences between the USPS and private couriers in training, public account-

[12] "In person," "by hand," "hand placed," and "thrown" are all distinct responses in the IS data and are included here as "in person or by hand." A replication of the identification of last mile suspicious-incident analysis for the explosives-related suspicious incidents is not possible using the IS data.

[13] In the database, a number of entries list simply town names for the location of detection, which may suggest that the suspicious item was detected at the town's Post Office or mail station. Under this assumption, that would push the estimate up to as high as 80 percent of IED and bomb-related suspicious items being detected at USPS facilities.

ability, and oversight. At the conclusion of this chapter, these issues are linked to the concrete examples of mail crimes just described, with projections for these crimes if the Mailbox Rule were to be relaxed.

Federal Regulations That Apply to Both the USPS and Private Couriers

Federal rules regulating the transportation of hazardous materials and employee occupational health and safety apply equally to the USPS and to private couriers. The Hazardous Materials Transportation Act of 1975 (as amended) and the U.S. Department of Transportation's (DOT) Hazardous Materials Regulations require any interstate, intrastate, or foreign carriers transporting hazardous goods through rail, aircraft, vessel, or ground vehicle to meet specified requirements, such as those that stipulate how such materials are packaged or labeled. These regulations define *hazardous materials* by type of material and detail the necessary standards for hazmat communication, such as requirements for shipping papers, markings, labeling, placarding, and packaging. They also detail requirements for emergency response plans in case of hazmat leaks or spills during transit, as well as security plans for safeguarding such materials from being tampered with or stolen.

In addition to communication requirements, the DOT's regulations require employers to provide hazmat training to all employees who handle or may be exposed to such goods. Employers must train hazmat employees, including general-awareness and familiarization training, function-specific training, safety training, and security training, depending on the employee's role and level of responsibility over handling such goods. Employees are required to receive this training every three years or when they change jobs. Hazardous-waste operations and emergency response (HAZWOPER) training requirements apply to the USPS and to private couriers.

The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has also issued standards about employee emergency plans and fire-response plans, hazmat storage and handling, and safety precautions and training requirements that employers must meet if they employ workers who handle or are exposed to hazardous materials. Every employer is required to have an emergency action plan

(EAP) that includes, at a minimum, procedures for responding to a fire or emergency, emergency evacuation, employees who remain for critical plant operations, accounting for employees after evacuation, and performing rescue or medical duties. Such plans must include the name or job title of every employee who may be contacted by employees who need more information about the plan or an explanation of their duties under the plan. OSHA also requires that an employer designate and train employees to assist in evacuating other employees.

OSHA further has implemented nonmandatory guidelines for handling anthrax and ricin, which were likely implemented in response to the anthrax attacks in 2001–2002 and the ricin scare in 2004. OSHA has provided guidance and standards for how employers should protect their employees and customers from exposure to biological agents in the workplace, bioterrorism, and specific toxic substances and hazardous materials, including bloodborne pathogens, air contaminants, and many other chemical and biological elements that may be hazardous to human health. Finally, OSHA provides guidance about compliance with its hazmat and hazard-communication standards and its emergency preparedness and response standards. Moreover, both the USPS and private couriers provide guidance to the public and to businesses on shipping hazardous materials and on what items are prohibited from their delivery networks.

Although we know in general with what regulations the USPS and private couriers must comply, we were also specifically interested in examining what type of training is provided on identifying and screening packages for suspicious or hazardous materials and what type of technology is being used to screen and detect such items.

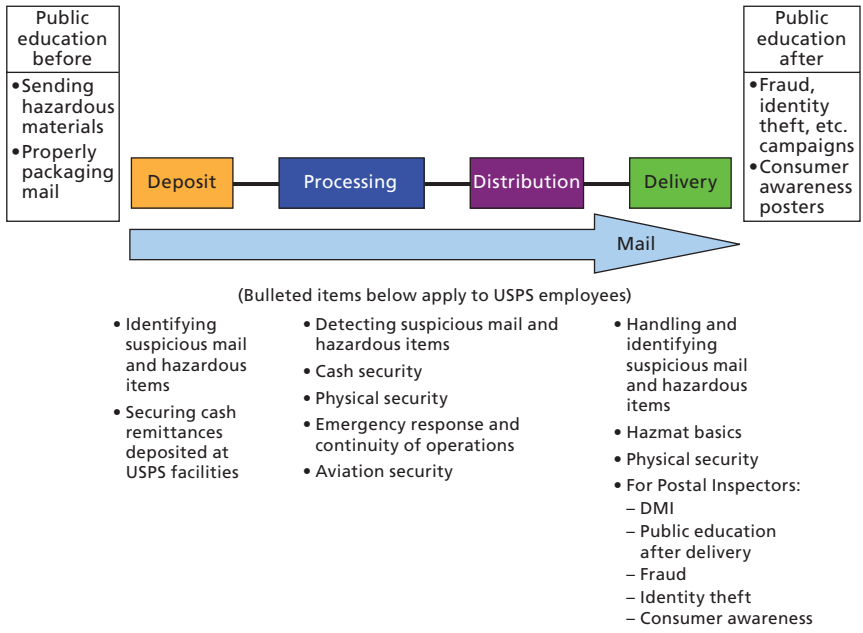
Differences in Training

We start by discussing what training the USPS and private couriers have in place. By *training*, we refer here to major training on mail security and detection measures for hazardous materials and suspicious items as well as to training on implementing guidance, policies, and procedures put in place. Training employees to handle the mail or items for delivery is central to the ability of the USPS and private cou-

rier companies to address and mitigate public safety and security risks, such as those discussed earlier.

USPS Safety and Security Training. USPS training is aimed at detecting and preventing mail crime, ensuring the security of the mail, and maintaining public safety. The safety and security of the mail at the point at which mail is deposited in a customer's mailbox depend on measures taken throughout each stage of the mailing process: collecting, processing, distributing, and delivering the mail to the USPS's 300 million customers (USPS, 2008a). As indicated in Figure 3.2, the majority of the training and security-detection measures apply to the processing stage, with some additional training, guidance, policies, and procedures applicable to the deposit and delivery stages. The distribution of suspicious-incident reports described earlier mirrors these training measures. The figure also shows that the USPS provides

Figure 3.2
The Postal System: Where Do USPS Training, Safety and Security Measures, and Public Education Campaigns Matter Most?



public safety education and awareness efforts to educate consumers about safety issues before they mail material and after they receive material.

Table 3.12 summarizes the guidance and training that the USPS and the IS currently use to promote the safety and security of the mail, their employees and contractors, and the public. Appendix C contains a more detailed presentation.

To protect the mail, the USPS has issued guidance about identifying and responding to suspicious- and hazardous-mail incidents, protecting cash sent through the mail, and protecting the mail from being stolen or tampered with. Moreover, the USPS has developed 142 employee-training courses, of which it actively conducts 114; these courses are not all focused strictly on safety and security measures. Of the safety- and security-specific training and guidance provided, the focus is particularly concentrated on identifying and responding to suspicious- and hazardous-mail incidents. For example, the USPS has 55 active courses that address hazmat procedures and awareness, of which four have been certified by the U.S. Department of Homeland Security (DHS); 42 active courses that address aviation mail security or security awareness in general; eight active courses that address handling suspicious mail or tabletop exercises for suspicious-powder incidents; and two active courses specific to anthrax in the mail (USPS staff, 2008). A total of 480,000 USPS employees have participated in these trainings; however, given that 75 percent of training is done by pay location, the data in USPS's National Training Database (NTD) do not permit us to break down the number of employees by type of training course.

In general, new city and rural carriers participate in a standard training course, which is intended to educate them about how to identify and handle damaged, suspicious, and hazardous mail. The course covers different methods for collecting mail, possible hazards, and procedures to follow when hazards or suspicious mail is identified. Letter carriers receive an update on this course as needed. HAZWOPER training is implemented every year as part of mandatory training. Managers and supervisors also deliver monthly mandatory talks to USPS employees nationally that focus on the use of SLAP guidance and the

Table 3.12
USPS Employee Guidance and Training

General Topic	Description
Guidance	
General employee training	Each employee receives a handbook specific to his or her assigned position. Besides addressing the basic work practices and responsibilities of the specific position, these handbooks may also address such areas as identifying and responding to suspicious or hazardous mail, keeping mail secure and protecting mail from theft or tampering, and physical security measures. Moreover, the USPS uses various forms of communication (such as its monthly publication, *Postal Bulletin*, and memoranda) to keep employees abreast of current postal security issues and updates in guidance or policies as well as to remind employees of existing policies.
Suspicious mail	The USPS has implemented a number of tools to keep employees educated and prepared for identifying, handling, and responding to suspicious mail or mail containing or believed to contain an unknown and potentially hazardous powder or substance. This guidance typically comes in the form of a poster, but it may also be presented as a training video or is included in general employee handbooks. Examples of posters include shape, look, address, or packaging (SLAP)[a] guidance on identifying suspicious mail; package, people, and plan (three Ps)[b] guidance on handling and responding to suspicious mail incidents; and, for higher-level employees, greater detail on how to respond to suspicious-mail incidents and whom to contact (i.e., the IS, local law enforcement, and local public health agencies) in the event that a piece of suspicious mail is identified.
Cash security	The USPS provides some basic posters and brochures for USPS employees who handle cash sent via the mail. These guidance materials address USPS recommendations for keeping the mail secure from theft as well as preventing mail crimes from occurring that place mail items at risk of being tampered with or stolen.
Hazardous materials	The USPS provides instructions on identifying and handling hazardous materials sent via the mail as well as guidance on identifying and responding to hazmat leaks and spills. These policies and procedures are generally provided in employee handbooks, posters, or brochures. They address such areas as what type of hazardous materials are permissible through the mail and in what amount; what hazmat symbols look like and mean; how to identify mail that may contain hazardous materials; how to handle packages that may be leaking hazardous materials; and how to respond and clean up such materials in the event that they may be leaking or may have spilled. The USPS has also implemented standard operating procedures for responding to hazmat spills and leaks; the procedures are provided to employees, especially managers and supervisors.

Table 3.12—Continued

General Topic	Description
Emergency response	The USPS has developed guidelines for developing EAPs and it requires each facility to have an EAP in place. To help supervisors and managers create such plans, the USPS has provided a checklist of items and issues to address in the EAP.
Physical security	Via handbooks, manuals, and memoranda, the USPS has issued guidance and mandatory requirements for physically securing USPS facilities and the mail. These instructions generally address measures that are required, such as wearing ID badges, enforcing ID badge requirements, keeping all doors locked, keeping mail that has either been collected and is out on delivery securely locked in appropriate receptacles, and following other mandatory physical-security requirements (e.g., outside facility lighting, surveillance equipment).
Training	
General employee training	When starting a new position with the USPS, each employee receives employee orientation training specific to his or her position. During such training courses, employees generally receive brief overview instructions related to identifying suspicious and hazardous materials. Some employees, such as sales and service associates and letter carriers, receive general instructions on keeping cash remittances and general mail safe from tampering or theft. Higher-level employees, such as postmasters, Postal Inspectors, PPOs, and management, may receive general training during orientation on emergency response.
Suspicious mail	All employees, regardless of level or position, receive basic training on identifying suspicious mail and mail containing unknown powders or substances. This includes the USPS's SLAP guidance,[a] three Ps,[b] and basic information on whom to contact in the event that suspicious mail or mail containing an unknown powder or substance is identified. Higher-level staff, such as managers and supervisors, receive more advanced training.
Cash security	As mentioned, during basic orientation, certain employees, such as sales and service associates and letter carriers, receive instruction about measures to take to protect cash remittances sent via the mail from theft. This training instructs such USPS employees to keep mail safely locked in appropriate places as well as to follow certain procedures that are intended to ensure continuous accountability for USPS employees of cash remittances.

Table 3.12—Continued

General Topic	Description
Hazardous materials	All USPS employees receive at least some basic ("awareness level") training in responding to hazmat spills and leaks (HAZWOPER training). Other, more specialized USPS employees, such as custodial personnel, supervisors, Postal Inspectors, and other persons designated to manage and clean up hazardous spills and leaks, receive more advanced (e.g., "operations level") HAZWOPER training. Other staff may receive even more advanced training, depending on the role that they are charged with playing during hazmat leak and spill response. The USPS also provides training to sales and service associates about the types of hazardous materials that are and are not permitted through the mail and the amounts of certain hazardous materials that are permissible. Certain USPS employees may also receive hazmat training specific to delivery crafts or aviation mail security. USPS staff in mail P&DCs receive training in handling mail containing hazardous materials to prevent contaminating the whole mail stream. Letter carriers are trained in handling mail containing or believed to contain hazardous materials and how to follow relevant hazmat procedures.
Emergency response	All employees are trained in basic facility emergency responses. Postal Inspectors and USPS facility employees participate in the Biohazard Detection System (BDS) alert response drills to prepare for possible BDS alerts. These drills also include local first responders and departments of public health. Higher-level staff, such as supervisors and managers, postmasters, and the like, receive, during basic training, instruction on how to respond to emergency situations, their role during such situations, and how to develop EAPs.
Physical security	The USPS provides basic physical security training to all staff who handle mail at any point during the mail collection, processing, or distribution stages. Such training includes educating staff about the necessity of wearing ID badges, keeping doors locked, and keeping all mail safely secured in appropriately locked places, such as a vehicle or a relay box. Other staff who are responsible for facility security, such as Security Control Officers (SCOs), receive more specific training regarding USPS policies relating to physical security.

[a] The SLAP guidance presents characteristics of suspicious mail in four easy-to-remember categories, based on the acronym SLAP: unusual shape, look, address, features, or packaging.

[b] The three Ps present three steps for responding to a suspicious package: (1) Package: don't handle it and isolate the area; (2) People: evacuate the area around the package and notify your supervisor; and (3) Plan: contact the IS, police, and community first responders.

three Ps (see Table 3.12), respectively, for identifying and responding to suspicious mail. In addition, informal safety talks and service talks are delivered on an ongoing basis.

In conjunction with the guidance and training mentioned, the USPS has implemented uniform recommended and mandatory policies and procedures for USPS employees to follow to protect the mail, USPS employees and contractors, and the public from hazardous events and mail crimes. In addition, the USPS uses its monthly publication (*Postal Bulletin*), its website, email, and memoranda as modes of continuous communication with employees on safety and security updates. These means of communication are used as an employee-education tool to update employees of any changes in guidance and policies, as well as to remind employees of existing guidance. For example, the USPS published regular updates on the anthrax response and what measures were being taken to protect USPS employees during the months following the initial anthrax attacks (USPS, 2001d).

Postal Inspectors also receive extensive training. In addition to basic inspector training, they receive training in responding to a biohazard alert, basic HAZWOPER training, and training on DMI. There are currently 340 DMI specialists nationwide within the IS. Their training includes the following phases:

1. 40 hours OSHA HAZWOPER, BDS evidence collection, and mail isolation, control, and tracking (MICT) training
2. 40 hours of forensic-sampling training
3. 40 hours of suspicious substance–screening training
4. 40 hours of pre– and post–bomb blast investigation training
5. 12 hours annual recertification. (USPS staff, 2008)

In addition, DMI specialists receive basic self-contained breathing apparatus (SCBA) training.

The USPS takes an all-hazards approach to emergency response.[14] Each of the 80 USPS districts has an emergency response team com-

[14] In FY 2007, the USPS reorganized its National Preparedness Office, placing it under the IS. This resulted in the expansion of IS emergency operations, with the addition of 81 homeland-security coordinators, nine national-preparedness managers, and an executive director of national preparedness (IS, 2008a).

prised of 18 primary and 18 alternative individuals.[15] Their focus is on emergency management and response for a disaster or emergency affecting USPS employees and facilities (e.g., how to lock down a facility in the event of a BDS alert). In addition to evacuation procedures for postal facilities, the USPS districts' continuity of operations plans address how to keep the mail moving in the event of a disaster.

How USPS Training Has Changed Since the 9/11 Terrorist Attacks. Before the 9/11 attacks, the USPS had various types of security training (including security training for special events such as the Democratic and Republican national conventions or major sporting events), as well as fiscal training for managers. However, mail security training was not mandatory at the national level; instead, it was left up to the local and district levels to determine what type of training should be made mandatory.

Since 9/11, the USPS has created a number of new courses to address the handling of hazardous materials (see Appendix C). Additional guidelines also were developed for employees on identifying and responding to suspicious mail, including mail that may contain biological or chemical agents such as anthrax or ricin (GAO, 2004a). In response to a review by the GAO (2005) and its recommended actions, the USPS expanded its training for managers and supervisors on handling and responding to suspicious-mail incidents and implemented revised mandatory guidelines for detecting and responding to mail that may be suspicious or contain unknown substances (GAO, 2005). This training became mandatory for all USPS employees—letter carriers, supervisors, managers, postmasters, and other mail handlers. Moreover, supervisors and managers are now required to participate in a Web-based training course on detecting and responding to suspicious packages and unknown, potentially hazardous powders or other substances sent through the mail. The USPS also was urged to provide more-explicit guidance to managers on communicating with employees and unions about suspicious-mail incidents (GAO, 2005).

[15] The emergency response teams are required to take four incident-command system online courses and a two-day course on BDS standard operating procedures, as well as participate in other on-site trainings.

Following the examination of lessons learned from the anthrax attacks and response, and in response to the GAO's recommendations for improving response to anthrax contamination (GAO, 2004a), the USPS published a Management Instruction outlining procedures to follow if the BDS generates a positive test and subsequent alert. The USPS also revised interim guidelines and emergency response guidance to better cover facility evacuation, personal decontamination, and the administration of postexposure antibiotics. Other adjustments included the development of an all-hazards emergency response plan for facilities (GAO, 2004b). In addition, the USPS created a National Emergency Preparedness Office and deployed emergency managers at major USPS facilities. Further, the USPS implemented related procedures and training of personnel in the event of an alert from the BDS, discussed in the next subsection.

Similar to the USPS, mail services in other countries also heightened security awareness following the 9/11 terrorist attacks. For example, Canada Post developed additional training materials and posters to address identifying hazardous materials and other suspicious items. Personal protective equipment (PPE), including gloves and masks, was made available to all employees and contractors. In addition, Canada Post's Security and Investigation Services conducted threat-risk assessments in its mail facilities. New Zealand Post similarly developed training to increase awareness and to address response to white-powder incidents and incidents involving possibly explosive devices.

Leveraging Technology to Ensure USPS Employees' and the Public's Safety. Anthrax spores sent through the USPS in 2001 and 2002 resulted in five deaths, 22 cases of anthrax, and widespread disruptions to the USPS (Gottron, 2002), including contamination of 23 USPS facilities (GAO, 2004a). In response to the anthrax attacks and given the post-9/11 security environment, the USPS implemented various technologies to ensure that the mail it processed and delivered would be safe from any hazardous materials that could harm USPS employees or the customers it serves. One of the key measures was the USPS's implementation in 2003 of its BDS, which detects biohazardous materials in mail at major processing centers (USPS, 2003). The BDS operates in conjunction with mail-canceling equipment, continually draw-

ing in air from the mail during the canceling process. The system tests air samples for possible anthrax contamination. More than 6.6 million BDS tests have been performed; approximately 30,000 tests are conducted weekly; and approximately 119 billion pieces of mail have been screened by the BDS since its deployment.[16] There have been no detected cases of anthrax contamination of the mail since the anthrax attacks in 2001 and 2002.

To protect employees, the USPS also installed air ventilation systems in its mail P&DCs to decrease the risk of biohazardous materials being dispersed through the air. In addition, the USPS has limited the use of compressed air to clean the processing machines to limit the risk of fine anthrax particles (or other potentially biohazardous powders) being dispersed throughout a processing facility (GAO, 2002a).

Safety and Security Training by Private Couriers to Protect Parcels and Express Mail. In the area of package delivery and other courier services, the most prominent companies include FedEx, UPS, and DHL.[17] In addition, there are other firms, such as regional and local couriers. We requested interviews with two of the major couriers operating in the United States to learn firsthand about the training, guidance, policies, procedures, and technology they currently use to protect the safety and security of their employees, their customers, and their deliveries. However, because we did not receive a response to our requests, we were limited to publicly available government and corporate documents to gain insights about the type of training and safety measures the major couriers have undertaken. Examining the security and training practices of smaller or local carriers was not feasible, given the time frame and scope of this study.

Private delivery carriers, such as FedEx, UPS, and DHL, have implemented measures to safeguard their service networks and their customers' packages. Each of the major couriers has expressed a com-

[16] Results of BDS testing as of May 8, 2008.

[17] FedEx is a courier service offering express small-package and document shipping. UPS is the world's largest small-package carrier, by revenue and by volume. Parcel services within the United States generate the majority of UPS's revenues, amounting to 62 percent or $30.98 billion in 2007.

mitment to promoting a safe and secure work environment for its employees and safeguarding its customers' packages. Beyond compliance with the mandatory federal regulations mentioned already, like the USPS, each major courier provides guidance to its customers on federal regulations about shipping hazardous or dangerous goods. This guidance is often provided in stores, on company websites, or through a company customer-service line that deals specifically with handling questions about shipping hazardous or dangerous materials. Although federal regulations require companies handling hazardous materials to have a hazard-communication program in place, some private companies have gone further by opening companywide communication mechanisms to allow for instantaneous communication with employees. For example, FedEx has established an internal website and television network that provide employees with workplace-safety information. It has also put in place a 24-hour hotline for employees to use if they have safety questions (FedEx, undated[b]).

As mentioned previously, some safety and security training is mandatory under federal regulations, such as OSHA and DOT regulations. Private companies may provide additional training beyond what is federally mandated, but we are unable to assess the degree to which this is done—with one exception. UPS invests more than $73 million per year in safety training and provides nearly 1.7 million hours of safety training annually. This includes 54 formal safety-training courses, which include but are not limited to training in hazmat handling, emergency evacuation, and hazard communication (UPS, 2008). These training courses are not *all* specific to promoting the safety and security of packages and may include general workplace-safety training, safe-driving training, or health-promotion activities.

The major private couriers also have in place security departments or safety committees to help identify potential risks and means of eliminating those risks. UPS, for example, has 2,900 Comprehensive Health and Safety Process (CHSP) committees across the nation to improve the health and safety of UPS employees. These committees consist of nonmanagement employees supported by management and are tasked with teaching employees how to identify workplace hazards, determining causes of hazards and accidents and injuries, recommend-

ing work processes and equipment to promote employee health and safety, and developing strategies to avoid injuries (UPS, undated[a]). FedEx also has implemented Safety Continuous Improvement Teams (similar to UPS's CHSP committees) that work to identify and alleviate safety risks (FedEx, undated[c]).

In response to 9/11, large firms, in general (including the USPS), undertook a number of steps to improve their preparedness and reduce their exposure to terrorism, such as planning for business continuity, developing more-extensive emergency response plans, assessing the security and vulnerability of their facilities and operations, adopting new security practices beyond industry norms, and redesigning supply chains to increase their security and resilience (Rice, 2003). In addition, although a unique example among the major private couriers, FedEx established a 10-person FedEx Air Carrier Police Department that is a fully certified law enforcement agency in the state of Tennessee, capable of carrying out its own investigations and allowing the company to participate in regional JTTFs (Fields, 2003; Block, 2005).

Identifying suspicious activity involving package-delivery systems has been a focus of at least one of the major private couriers. FedEx has encouraged its employees to report unusual activities or potential terrorist activities to its police force, has provided its package-processing employees with pocket guides about identifying suspicious packages, and has instituted a special computer link that allows reports of suspicious activities to be sent directly to the DHS. Moreover, FedEx uses its extensive international database in collaboration with the FBI to flag suspicious packages for additional inspection (Block, 2005). Finally, FedEx has installed radiation detectors in its foreign facilities to detect dirty bombs (Block, 2005). We found no other public documents indicating similar efforts by the other private couriers.

Although the preceding discussion provides some insight to the safety and security activities of the major private package-delivery carriers, it is a very basic snapshot of what is currently being done. Because we were unable to speak directly with safety and security representatives from FedEx, UPS, or DHL, our analysis relies heavily on what is known about federal regulations that apply to *all* private courier companies and any literature or information that is available through corpo-

rate documents, literature, and the Internet. This limited our ability to provide detailed summaries of the safety and security training, guidelines, and policies and procedures that private carriers have in place. In particular, we were unable to assess training provided to employees by level of employee; hazardous- or dangerous-materials training beyond what is federally required; suspicious-package training and guidelines available to employees; and training, guidelines, and policies and procedures to promote the physical security of packages delivered through private carriers. We also were unable to identify technology used by private carriers other than FedEx. Further, we did not assess state or international regulations that may apply to package-delivery carriers.

We can assume, however, that private companies are likely motivated to implement safety and security measures to minimize the threat of business disruption. For example, a hazmat leak or spill may interrupt the flow of packages through a private company's delivery channel and, thus, harm its ability to meet business goals. Moreover, we assume that shareholders hold private-sector companies accountable and that these companies therefore feel some pressure to safeguard their employees and their primary product, the express delivery of packages.

Concerns About Training Differences for Public Safety and Security. If the Mailbox Rule were to be relaxed, private courier services, including the major carriers as well as smaller local and regional carriers, would have access to the mailbox. A key concern is what type of training private couriers—in particular, smaller local and regional couriers—provide their personnel in terms of identifying suspicious or hazardous items. In general, smaller employers are less likely than larger firms to provide formal training programs for their employees (Lynch and Black, 1995). As discussed earlier, much of the USPS's training and other security measures (e.g., technologies such as the BDS) is concentrated on the processing stage with the aim of detecting suspicious or hazardous items before they reach the mailbox. Supporting evidence from our "last mile" analysis of the incident data suggests

that the USPS may have more-sensitive detection of suspicious items in place than do private courier companies in general.[18]

Another concern is the effect of differences in attrition rates on training. Higher turnover rates in personnel are expected to have implications in terms of a firm's ability to keep its personnel trained. The USPS and UPS have relatively low annual employee-turnover rates, approximately 4 percent, which works in favor of ensuring that employees are adequately trained. However, the UPS turnover rate is far below industry standards. For example, FedEx has a voluntary turnover rate of approximately 9 percent ("100 Best Companies," 2008). One might expect that smaller courier firms may have higher turnover rates, making it more challenging to keep personnel trained and more difficult to ensure that they meet basic training standards. Most couriers receive their training on the job, training with an experienced worker for a short period of time (BLS, 2007).

Finally, the delivery channel for the major private couriers differs from that of the USPS in some important ways that may have implications for training and the types of risks private couriers may face. For example, both USPS carriers and UPS drivers are assigned specific routes. However, the USPS carrier will have a daily presence throughout a neighborhood or delivery route. Although UPS drivers have assigned routes, the frequency with which the driver interfaces with individual businesses or residents on the route will vary considerably. In this sense, USPS carriers may be more likely to have a more detailed knowledge of what is occurring on their route and ability to identify whether anything is out of the ordinary. The size of the USPS and UPS delivery networks varies substantially, and the number of customers with whom they are in contact on a daily basis also varies.

---

[18] The suspicious-incident data include a number of items that originated from non-USPS carriers but entered the USPS delivery chain at some point, such as last mile deliveries. These items were not identified as suspicious by the non-USPS carriers, but were identified as suspicious before delivery at a higher rate than were items that originated in the USPS delivery chain, suggesting that the private couriers handle, and detect less frequently, items that the IS considers suspicious. Thus, we expect that there may be greater variability between the USPS and private couriers (especially among the smaller carriers) in the processes and procedures in place to screen material, including packages and documents.

For example, as noted earlier, the USPS delivers mail to 300 million people at 148 million homes, businesses, and Post Office Boxes (USPS, 2008a). In comparison, the number of daily customers UPS services is estimated at 7.9 million daily (1.8 million pickup and 6.1 million delivery) (UPS, undated[b]).

Differences in Oversight and Accountability Mechanisms

Related to the issue of differences in training are differences in oversight and accountability mechanisms. The USPS has a number of accountability mechanisms, including the USPS Office of Inspector General (OIG), the USPS Board of Governors, the Postal Regulatory Commission (PRC), Congress, and the GAO.[19] The OIG, for example, is responsible for conducting internal audits, reviews, and investigations of USPS programs and operations: (1) to prevent and detect fraud, theft, and misconduct; (2) to promote economy, efficiency, and effectiveness; and (3) to promote program integrity. The OIG is also responsible for keeping governors, Congress, and USPS management informed of any problems and corresponding corrective actions. The PRC is an independent agency, established in 1970 by the Postal Reorganization Act, with regulatory oversight of the USPS. The PAEA, enacted in 2006, strengthened the PRC's authority and assigned new and continuing oversight responsibilities including review of the Universal Service requirement, annual determinations of the USPS compliance with applicable laws, and development of accounting practices and procedures (Postal Regulatory Commission, undated). Importantly, the GAO has conducted external reviews of USPS training and policies and procedures in such areas as cash security and guidance related to handling of suspicious mail and hazardous materials. Since 2000, the GAO has published a series of reports examining many aspects of the USPS's role and operations. The GAO has conducted assessments of the USPS's ability to effectively and efficiently detect and respond to threats such as suspicious mail, anthrax, and other biohazards, as well as to protect the physical security of the mail and of cash remittances

[19] The GAO is an independent, nonpartisan, federal agency that works for Congress investigating how the federal government spends taxpayer dollars.

sent through the mail. In each of the GAO's comprehensive evaluations, it provided a critique of USPS guidance, training, and policies and provided recommendations to improve such safety and security measures, many of which have been adopted.

Oversight and accountability mechanisms arguably vary between the USPS and private-sector couriers. Unlike the USPS, private-sector companies are not directly accountable to taxpayers. Beyond an internal-control office, private courier companies do not necessarily have formal accountability agencies like the USPS has in the federal government's GAO. Private-sector companies, however, are required to meet federal regulations, as mentioned earlier (e.g., OSHA standards, DOT regulations, Federal Aviation Administration [FAA] regulations, U.S. CBP requirements). Moreover, publicly traded private companies, such as FedEx and UPS, are accountable to their shareholders. We mentioned in Chapter Two that private couriers participate in several federal programs—in particular, the NIPP and C-TPAT. However, participation in these programs varies widely, especially among the smaller couriers. Further, C-TPAT has been criticized for being behind in verifying that participating members' security practices meet the minimum established criteria (Stana, 2005).

Concerns About Oversight and Accountability Differences for Public Safety and Security. Based on these differences among the USPS, publicly traded companies like FedEx and UPS, and privately owned local and regional courier companies in terms of oversight and accountability, we would anticipate that relaxing the Mailbox Rule would raise concerns regarding training standards, suspicious-item detection technology, and hazardous materials handling. In particular, it would raise the question of what training standards should be required of all couriers and what policies and procedures for handling hazardous materials or suspicious items, for example, will need to be established. It would also raise the question of who will enforce such national standards and how they will be funded. Ensuring that *all* carriers, public and private, have the necessary training, guidance, and policies in place will require federal, state, and local enforcement of standards that regulate such measures. The measures should cover training on detecting and handling hazardous materials and suspicious items, detection of potential

fraud items (such as Nigerian fraud letters), and reporting and responding to such incidents. In addition, one would need to determine what constitutes a reasonable level of effort for doing so. As a result, additional federal, state, and local spending and resources may be needed to enforce such standards. Of course, if customers have concerns about the type and number of incidents associated with certain couriers, they may stop sending packages through those couriers.

Security Implications of Relaxing the Mailbox Rule

Having established the types and number of security incidents and trends from 2003 to 2007 and having examined issues of differences in training and in accountability and oversight that could have an impact on public safety and security if the Mailbox Rule were to be relaxed, we now turn to the implications of doing so. We first discuss some general implications, before returning full circle to look at the more specific implications by the categories of incidents described at the beginning of the chapter.

General Implications of Relaxing the Mailbox Rule

Any discussions about changes to the Mailbox Rule must include a clear understanding of the safety and security consequences related to such changes. Currently, the USPS collects, processes, and distributes the majority of U.S. deliveries, and it processes and delivers approximately 2.8 billion pieces of international mail annually (USPS, 2008a). Removing the Mailbox Rule could eventually reduce the amount of mail that the USPS processes and delivers. The experience of the United Kingdom, where the Royal Mail was privatized and the market completely liberalized in 2006, is one example of such a change. The Royal Mail experienced a 20-percent decrease in the total upstream market and similar (if not more) decrease in bulk mail sent by businesses to other companies and domestic consumers (Hooper, Hutton, and Smith, 2008). However, as was the case for the Royal Mail, the USPS would likely retain nearly all the letter volume in the United States in the near term. One hypothesis put forth by the USPS is that,

although the USPS may retain most of the letter volume in the near term, public security concerns may have a negative impact over the long run, resulting possibly in electronic diversion of some volume, such as bill-paying, banking, or check-depositing.[20] It also underscores possible public concerns that security may be affected. We discuss public security concerns in more detail in Chapter Five.

If the USPS has less control over the mail sent through its system, which includes both private and public mail-delivery services, other non-USPS entities may be charged with safeguarding additional mail volume and protecting employees and the public from mail crime.

Opening the mail-carrying market to private carriers would likely result in an increase in the number and variation of carriers delivering mailable matter without postage to the mailbox. As a result, it may become increasingly difficult to identify who is legally allowed access to the mailbox, which has implications for identifying individuals with such authority, as well as for granting access to otherwise secure buildings, such as apartment buildings or offices. Ensuring that granting access to secure buildings to individuals whom tenants may not be able to identify does not breach security implies that standards need to be set about properly identifying individuals legally allowed access to buildings and mailboxes. Opening up the mail market to private competitors raised the issue of registration of couriers in New Zealand. Moreover, it highlights the need for private and public couriers to require background checks for employees who would be accessing secure buildings and mailboxes.

Allowing non-USPS entities access to the mailbox increases the potential for unsafe deliveries. Thus, the USPS may need to implement additional training for its letter carriers about identifying and responding to suspicious or hazardous deliveries placed in a mailbox by an entity other than the USPS. Additional training in this regard would

---

[20] Although the impact of relaxing the Mailbox Rule or the Postal Monopoly is expected to be less on letter volume, the effect may spill over to letter volume. First-Class Mail (single-piece letters and bulk mail) volumes and Standard Mail volumes are on the decline (President's Commission on the United States Postal Service, 2003). This, in theory, could accelerate the electronic diversion of First-Class Mail and Standard Mail to cheaper, Internet-based alternatives.

require more USPS time and resources. New Zealand Post is virtually the only entity that provides end-to-end service in that country, with most competitors giving their mail to Post for actual delivery. At times, dangerous goods (hazardous materials) prohibited by New Zealand Post have come through its network from third-party suppliers. To address this problem, the approach New Zealand Post has taken is to work with its competitors to improve their processes so that dangerous goods do not enter the network. Although effective in New Zealand, this strategy may not be feasible in the United States because of the sheer size of USPS's networks and the potential for numerous competitors in the market of varying capabilities in their screening processes and procedures.

Although the USPS and IS are heavily invested in public awareness campaigns to prevent mail crime and its severity, tight budgetary constraints may affect their ability to continue to invest in such efforts. For example, if the IS cuts back on its investigations either because of decreased investigative authority or because private companies do not contact it when mail crimes occur, it may have less funds to put toward public education and awareness campaigns.

Relaxing the Mailbox Rule: Implications for Security Incidents

Here, we discuss the possible effect of relaxing the Mailbox Rule on each of the five categories of incidents discussed at the beginning of the chapter. We would anticipate that a key effect of opening up access to the mailbox would be that more individuals having access to them would create more opportunities for mail theft. Thus, the main risk to the public might be in terms of theft at the mailbox, including identity theft, credit-card theft, and theft of pension checks or other payments. This would be a particular concern if relaxing the Mailbox Rule led to fewer locked mailboxes.

Implications for Volume Attacks. Volume attacks are essentially large-scale mail thefts, most commonly those against multiple-mailbox receptacles such as apartment panels, CBUs, and NDCBUs. The extent to which relaxation of the Mailbox Rule would affect the number of volume attacks would depend on how the relaxation is implemented. Because of the logistical complexity of providing keys to locked mail-

boxes to all private courier companies, it would be anticipated that locked mailboxes would essentially remain subject to a de facto Mailbox Rule, such as exists in Canada. Hence relaxing the Mailbox Rule would not increase opportunities for volume attacks, at least so long as locked mailboxes remain subject to a de facto Mailbox Rule.

Implications for Fraud. We would anticipate only a weak relationship between relaxing the Mailbox Rule and changes in the incidence of fraud.

As captured by the IS data, fraud involving the mail is usually detected after delivery,[21] either after the initial contact letter through the mail itself or when expected products or services arrive in the not-as-advertised state (if they arrive at all). For most frauds using the mail, the concern is generally not who is accessing the mailbox or who is delivering what types of items, but rather what happens after delivery. Fraud involving the mail generally cannot be detected until the fraud occurs, although some types of frauds are evident on the face of the mailings (e.g., Nigerian fraud and mailings from known fraudsters). (Only 2 percent of all victims reported that the theft of their identity was connected to the mail; see FTC, 2007.)

Relaxation of the Mailbox Rule could affect the incidence of the largest category of fraud reported to the IS—merchandise or service fraud[22]—if opening up access to the mailbox increases the risk of mail theft, making nonfraudulent merchandise seem fraudulent (i.e., nondelivered). Theft from the mailbox would become increasingly conflated with merchandise fraud, making it difficult to know whether a given case is fraud or mail theft. Under this scenario, urban areas would be most affected because of the greater potential for theft (essentially the same as the impact on mail theft).

To the extent that some types of frauds in the mail can be detected prior to delivery, diversion of mail to private couriers resulting from

---

[21] As opposed to fraud that occurs through other means. For example, some fraud may be detected when a bank's or retail company's computer-security systems are hacked.

[22] Currently, merchandise and service fraud comprises 31 percent of reported incidents in which the IS opens a case or makes an arrest. The need to establish whether items were delivered but then stolen or actually fraudulent (never delivered) would decrease the IS's ability to pursue the same level of merchandise and service fraud detection that it currently does.

relaxing the Mailbox Rule might hamper fraud detection because non-USPS employees are not as well trained as USPS employees are. For example, the USPS trains its personnel to recognize the characteristics of Nigerian fraud letters; however, non-USPS personnel are, at least currently, probably less likely to be trained in detecting this type of fraud. The rapidly growing significance of Nigerian fraud (12 percent of all fraud in 2007 and one of the types of fraud with the highest median dollar loss to victims) might be partially mitigated through provision of USPS training modules to private couriers.

In addition, once detected, the IS has the authority to stop mail under 39 U.S.C. §§ 3001–3009. The IS also uses its Administrative Action program and its cooperation with CBP and foreign law enforcement agencies to prevent mail from being delivered. In 2007, the IS seized and destroyed 309,000 pieces of illegal foreign lottery mailings under this program (IS, 2008a).

Implications for Financial Crime. Financial crime reported to the IS primarily involves mail theft of some kind. To the extent that relaxing the Mailbox Rule might increase mail theft because more individuals would have more opportunities for mail theft, financial crime predicated on mail theft might increase.

Urban areas may be affected to a greater extent, both because they already are disproportionately victimized by mail theft and because more densely populated areas put more people in proximity to mailboxes. Rural areas may have an additional protective factor in the USPS last mile delivery service of non-USPS items, limiting the number of people delivering to the mailbox.

The key issue with the financial crime that the USPS monitors (listed in Table 3.6) is not what goes into the mailbox by what method (which is dictated by the PES more broadly), but rather who can access the mailbox to remove items (which is dictated largely by the Mailbox Rule). Relaxing the Mailbox Rule would thus likely be associated with an increase in the incidence of financial crime, primarily through mail theft. The financial crime considered here that is not linked to theft from the mailbox, such as using the mails in the furtherance of such crimes as passing counterfeit checks, is rarely detected by the USPS during its delivery process. Thus, having such items travel through

another carrier might have little impact. If higher-income areas see the largest change in who delivers to them, the increased traffic could lead to disproportionate increases in fraudulent applications and identity theft. Here again, rural areas may see a security advantage stemming from USPS last mile delivery.

Implications for Suspicious Incidents (excluding IEDs and bombs). For suspicious incidents, relaxation of the Mailbox Rule is important. Trends for the incident data suggest either that the IS is responding to a real rise in suspicious items with greater success (predelivery identification) or that increasingly sensitive detection methods are capturing suspicious items that were not previously detectable (or a combination of both). In either case, training plays an important role, as does technology. Further, as discussed in our last mile analysis, the limited evidence suggests that the USPS is more sensitive in detection than other carriers are. Relaxing the Mailbox Rule would likely result in an increase in the number of suspicious items that are delivered to customers by private couriers. This problem is likely to be heightened for urban residents more than rural residents if non-USPS carriers concentrate more in the urban areas. Of course, most suspicious items are false positives presenting no safety risk, although some may cause fright to the customer and result in an investigation.

Implications for IED and Bomb Incidents. We would anticipate two ways in which relaxing the Mailbox Rule might increase the number of IED/bomb incidents. First, as just described with regard to suspicious incidents in general, if detection training and technology vary among the different private carriers, there might be variability in their ability to detect parcels that could contain an IED. Second, if the Mailbox Rule were relaxed to the fullest extent, resulting in fewer locked mailboxes, there would be more opportunities for hand delivery of an IED/bomb.

Urban and Rural Differential Effects on Security of Mail and Public Safety. As described, there are some differences between urban and rural areas in their experience of various types of incidents. For example, financial crime is disproportionately a larger problem in urban areas, while rural areas were disproportionately more likely to have suspicious items identified after delivery. Given that the USPS has

in place a myriad of measures to safeguard the mail, its employees, and its customers, customers who reside in areas that are not likely to be served by private carriers (rural and high-crime areas) may actually be at less risk of increase for certain types of mail crime—in particular, suspicious or hazardous incidents involving the mail.

Summary

Currently, the USPS and IS are doing much in the area of training focused on enhancing public safety and security. Given the range and types of incidents and threats to mail security, their training appears to be appropriately focused.

Based on our analysis, we would anticipate that the main effects on public safety and the security of the mail stemming from relaxing the Mailbox Rule may be (1) increased theft at the mailbox contributing to financial crimes, such as identity theft, credit card theft, or theft of pension checks or other payments; (2) increased risk of suspicious items getting through the processing phase and being delivered to consumers by private couriers; and (3) increased risk of bombs or IEDs being delivered by private couriers and possibly by individuals. Of course, it is difficult to assess the current baseline level of risk from which these increases might occur. For instance, the nature of the reporting that underlies IS data collection likely underestimates the true level of financial crimes substantially, while suspicious-incident detection catches few true positives. Other risks, such as bombs and IEDs, which are likely measured much more accurately, indicate relatively low risk to individuals on a national level.

Accordingly, based on the limited data available, we would speculate that the magnitude of the increase of mail theft would likely be moderate, since more people will have access to the mailbox (and thus, more opportunities for mail theft). Such an increase would be contingent on the degree of relaxation, particularly whether only the major couriers or a wider range of different types of couriers are allowed to enter the postal market and whether private couriers are granted access to locked mailboxes. In addition, we would also anticipate greater vari-

ability in personnel training. This suggests that USPS personnel (and IS personnel, as discussed in Chapter Four) may require additional training. That is, there may be an increased need for training on the USPS side to address a wider range of events happening at the point of delivery.

These changes raise a fundamental question of whether training standards should be set as part of the decision to open up access to the mailbox. If so, who will be responsible for enforcing them and ensuring that they are met?

In Chapter Two, we noted that it is unlikely that relaxing the Mailbox Rule would result in the decision to open up access to locked mailboxes, such as apartment panels. As we discuss in Chapter Five, approximately 26 percent of the population has locked mailboxes. In this analysis, we did not explicitly examine the issue of how opening up access to the mailbox might be done or the cost of doing so. We point out only where we believe that there may be an increase in incidents if mailbox access were opened up. Like Canada, one option the United States has in relaxing the Mailbox Rule would be to maintain the locks on mailboxes currently in place, allowing only the USPS to control access and making it a criminal offense to be in possession of the keys, not just to steal or reproduce the keys (as provided by 18 U.S.C. § 1704).

Finally, rural and lower-income areas might experience less negative public safety effects from relaxing the Mailbox Rule than would urban and higher-income areas because of smaller shifts toward delivery by private courier services for these groups because of cream-skimming and the availability of the USPS last mile service (see, e.g., Lacker and Weinberg, 1998).

CHAPTER FOUR

Relaxing the Mailbox Rule: Effect on the IS's Ability to Detect, Deter, and Investigate Crime

Following the previous chapter's analysis of reported security incidents and the potential changes in security-incident patterns that might follow relaxation of the Mailbox Rule, we now turn to the question of how relaxing the Mailbox Rule might affect the policing of mail crimes. This chapter discusses what impact relaxing the Mailbox Rule might have on the IS, the law enforcement agency with primary responsibility for investigating crimes involving the mail, and its ability to deter, detect, and investigate crimes involving the mails.

As mentioned in Chapter Two, the IS enforces nearly 200 laws that make a wide variety of acts federal crimes if they involve the U.S. mail or other USPS services. Some of these crimes are focused on the mail itself, such as mail theft, obstruction of the mails, and destruction of mail. Some are focused on the infrastructure of the postal system, such as destruction of the mailbox or mail depositories, assault or robbery of USPS workers, or theft of or fraud against USPS resources. These criminal statutes empower the IS to protect the USPS and the postal system. Other statutes provide federal jurisdiction for specific "regular" crimes, such as fraud, identity theft, child pornography, and conspiracy to commit a crime, when the mail is used in furtherance of the crime. Many of these latter statutes also provide federal jurisdiction when the crime has a connection to interstate commerce, but, in such situations, federal law enforcement agencies other than the IS will likely have investigative jurisdiction if mail is not involved in the crime.

The IS contends that relaxing the Mailbox Rule would limit its powers to investigate crimes because the USPS would lose jurisdiction over the mailbox and that mail that is diverted to private couriers will

not be subject to its jurisdiction, even if there is an interstate commerce basis for federal jurisdiction. Further, the IS asserts that not only will the costs and complexity of its investigations rise, but it will lose its current ability to track mail crimes, and its ability to deter crimes will be frustrated. This chapter assesses each of these arguments in turn. The arguments discussed here are based on a series of personal communications with IS staff.

Relaxing the Mailbox Rule: Effect on Federal Jurisdiction Over Mail

"Mail" and the Mailbox

The IS contends that relaxing the Mailbox Rule will reduce federal criminal jurisdiction over USPS deliveries and the mailbox. Of the approximately 200 sections of the U.S. Code that establish federal mail crimes, several protect mail in the mailbox and the mailbox itself. These include obstruction of correspondence (18 U.S.C. §§ 1701 and 1702), destruction of letter boxes or mail (18 U.S.C. § 1705), and theft or receipt of stolen mail (18 U.S.C. § 1708), as well as deliveries without postage—the Mailbox Rule itself (18 U.S.C. § 1725).[1] These apply to the mailbox because the USPS has established the mailbox as an "authorized depository of mail matter" pursuant to its authority to issue regulations to "establish, approve, or accept" any letter box "for the receipt or delivery of mail matter on any mail route" under the Mailbox Rule statute, the mail-theft statute, and 39 U.S.C. § 401 (general powers of the USPS).

The IS argues that relaxing the Mailbox Rule would reduce federal criminal jurisdiction over USPS deliveries to the mailbox and over mailboxes themselves, based on the assertion that relaxing the Mailbox Rule would render policing the mailbox difficult because many other

[1] The IS contends that relaxing the Mailbox Rule would also reduce federal jurisdiction for several other mail crimes, including sending sexually explicit materials (18 U.S.C. § 1735, 39 U.S.C. § 3010), explosive devices and nonmailable hazardous material (18 U.S.C. § 1716), firearms (18 U.S.C. § 1715), child pornography (18 U.S.C. § 2252), and mail-fraud schemes (18 U.S.C. § 1341 et seq.). These are discussed in the next section.

entities would routinely make deliveries to (at least unlocked) mailboxes. As a result, letter carriers' efforts to pick up outgoing mail and conduct business at the mailbox would become more complicated, and the USPS would effectively lose control over the mailbox. In addition, as discussed in the next section, diversion of mail to private couriers would require the USPS to share jurisdiction over the mailbox with numerous law enforcement and regulatory authorities. Accordingly, the IS argues that relaxing the Mailbox Rule would make it impossible for the USPS and the IS to control the mailbox.

Without control of the mailbox, the IS argues that the USPS would need to treat the mailbox like it treats mail slots. USPS regulations have excluded mail slots in front doors, as well as nonlockable bins or troughs used in apartment buildings, from the category of "authorized depositories of mail matter" (DMM 508.3.1.2). The logic underlying the exclusion of mail slots is obvious. Unlike the access it has to the mailbox, the USPS has no access beyond the mail slot, and mail slots cannot be as easily used to send outgoing mail or to conduct USPS transactions.

The IS also asserts that relaxing the Mailbox Rule would force the USPS to cancel the status of the mailbox as an authorized depository of mail matter because the USPS could no longer exercise exclusive control over the mailbox and it would incur heightened costs to secure U.S. mail in a shared mailbox. If the mailbox is no longer an authorized depository, it would no longer be protected under the federal statute prohibiting destruction of letter boxes. Destruction of the mailbox would become a state matter, and the IS would have no investigative involvement.

In the IS's view, ending the mailbox's status as an authorized depository would change the point at which many USPS deliveries cease to be "mail." The USPS is responsible for the security of the mail only while it is mail—that is, while it is under USPS control. Once delivered to the addressee's or agent's hands, it ceases to be mail and becomes mere property. Mail delivered to an authorized depository remains mail until the addressee or agent retrieves it, whereas mail delivered to mail slots ceases being mail on delivery because it is in the addressee's control. This is relevant because statutes governing crimes

against mail apply only while the delivery is still mail.[2] Hence, destruction or theft of mail is a federal crime only while the delivery is mail. Once it is delivered, destruction or theft of the item becomes destruction or theft of personal property under state law, and the IS would have no investigative involvement.

It is clear from discussions with IS officials that having more players in the mailbox, in their view, will likely make the jobs of the USPS and IS more complicated and more costly. Although this monograph does not address how relaxing the Mailbox Rule might affect USPS operating costs, we discuss later how it might add complications to IS investigations, which, in turn, could have cost implications. If costs were to rise because of relaxation of the Mailbox Rule—which would seem likely, although by how much is unclear—this might cause the USPS and IS to shift their funding resources and priorities unless relaxation were offset by an appropriation.

It is not clear whether the USPS would be forced to cancel the mailbox's classification as an authorized depository of mail matter. Even if costs were to rise, the USPS and IS could adjust their funding priorities. However, this may not be feasible given that the USPS has experienced a multibillion-dollar loss in FY 2008 and expects a multibillion-dollar loss in FY 2009 and FY 2010 as well. One option would be to cease picking up outgoing mail, at least from locations near USPS blue collection boxes. Another option would be for Congress to mandate that the mailbox continue to be an authorized depository so that U.S. mail delivered to the mailbox retains its status as mail. The mailbox-rule statute and Title 39 of the U.S. Code grant the USPS authority to determine what depositories are authorized to receive mail. Hence, the USPS has the power to alter the definition of *authorized depository* as it sees fit, except to the extent directed by Congress. A congressional mandate would allow federal mail statutes to continue to protect U.S. mail in the mailbox as well as mailboxes themselves (but not to attacks against private courier deliveries in the mailbox, such as

[2] Federal statutes about crimes committed *through* the use of the mail (such as mail fraud or sending hazardous material) as opposed to *against* specific items of mail (such as mail theft or destruction) do not have this temporal element.

theft or tampering), and the IS could still investigate. This approach might also entail a rise in IS operating costs, which Congress could offset with an appropriation.

It is also not clear what the public safety impact may be if the IS no longer policed the mailbox. There are no existing data to compare the relative security of mail slots and the mailbox. The IS argues that state and local law enforcement agencies likely will not investigate most mailbox crimes, such as mail theft, because they focus their resources on violent crimes. Based on the experiences of other countries, there could be some merit to this argument, as discussed further later. However, it is worth noting that less than 1 percent of mail-theft reports result in an arrest by the IS, as discussed in the deterrence section below. Of course, many mail theft arrests are for volume attacks (each one of which may account for many mail theft complaints) and the IS works with state or local law enforcement to prosecute some cases that the U.S. Attorney will not accept. In addition, some states, such as California, have passed laws enabling state and local law enforcement agencies to investigate and prosecute mail-theft crimes to alleviate the IS's caseload, as well as criminalizing or increasing criminal penalties for identity theft–related fraud (Office of the Governor of the State of California, 2006).

To the extent that the loss of the IS's power to police the mailbox would affect security, it would most likely be felt in removing the only specialized law enforcement agency in the United States from its area of expertise and from its ability to act across local and state jurisdictional lines. For instance, although the IS conducts investigations in individual small crimes, it has a strategic focus on large crimes, such as mail-theft, identity-theft, and fraud rings. IS concentration of mail-theft resources on mail-theft rings or mail thieves who attack CBUs has had great effect. As discussed in the section on deterrence, the IS reports a 35.7-percent reduction in volume mail attacks from FY 2006 to FY 2007 (IS, 2008c, pp. 17–18). Its personnel are highly experienced in this area, have developed nationwide institutional knowledge that allows them to identify criminal tactics and patterns, and can share information seamlessly, unlike geographically based law enforcement

agencies. Relaxing the Mailbox Rule might limit IS involvement to providing technical assistance through a multiagency task force.

In addition, the IS (through the USPS) can make the wider public aware of threats. For instance, in response to the attacks by Lucas John Helder, the "Smiley Face Bomber" in 2002 (so-called because he intended to bomb mailboxes in locations that would form a smiley face across a map of the United States), the USPS sent notifications to its customers across many jurisdictions urging them to leave their mailbox doors open so that they could see whether a beverage bottle–based IED had been left in their mailboxes. (The culprit was arrested after a joint investigation involving the IS, the FBI, and state and local law enforcement agencies; see IS, 2002, 2004f.)

Unlike the United States, both Canada and New Zealand have national police forces with varying responsibilities in investigating mail-related crime. Canada Post's Security and Investigation Services works closely with law enforcement to detect and investigate crime when it deals with incidents that occur in the "course of post." (Mail-theft crimes that occur after delivery are the purview of local law enforcement.) New Zealand Post's security team is deployed across its network. It will bring to law enforcement's attention possible cases of mail crime for investigation. In general, given the level to which law enforcement agencies are underresourced, there can be some variation in the priority that law enforcement gives to mail theft because of competing priorities for limited police resources.

Diversion of Mail to Private Couriers

In addition to possibly limiting federal jurisdiction over crimes committed at the mailbox against mail delivered by the USPS or against a mailbox itself, discussions with the IS indicate that the IS is concerned that the diversion of mail to private couriers will take diverted deliveries outside of the IS's investigative jurisdiction. The USPS contends that relaxing the Mailbox Rule would divert some proportion of USPS mail-flow (less than 26 percent, as discussed in Chapter Two) to private courier companies. Because federal mail-crime statutes apply only to "mail" (i.e., USPS deliveries), diversion would take crimes committed

using or against private courier deliveries outside the reach of federal mail-crime statutes and IS investigation.

Some federal mail-crime statutes also apply to deliveries in interstate commerce. Congress has provided federal jurisdiction for several types of crime by pinning federal jurisdiction on *either* the use of the mails *or* interstate commerce in furtherance of the criminal act. Examples include mail-fraud schemes (18 U.S.C. § 1341 et seq.); sexual exploitation of children (18 U.S.C. § 2251); child pornography (18 U.S.C. § 2252); the visual representation of sexual abuse of children (18 U.S.C. § 1466A); use of interstate facilities to transmit information about a minor (18 U.S.C. § 2425); enticing minors into sexual activity or prostitution (18 U.S.C. § 2422); the use of weapons of mass destruction (18 U.S.C. § 2332a); sending communication-interception devices (18 U.S.C. §§ 2511 and 2512); counterfeiting (18 U.S.C. § 2318); murder for hire (18 U.S.C. § 1958); and stalking (18 U.S.C. § 2261A). Of course, these statutes provide federal jurisdiction only where an actual interstate commerce nexus exists in the crime. Acts committed entirely within a single state have no interstate commerce jurisdictional hook, which means that state law applies. Either way, the IS argues that it would not be able to investigate these crimes because it has no investigative jurisdiction over nonfederal crimes, and it investigates only federal crimes that involve the mail. Hence, there would be a loss of IS expertise, except to the extent that the IS can provide technical support through a multiagency task force. Not all mail crimes have an interstate commerce alternative. The statutes discussed in the preceding section—mail theft, obstruction of correspondence, and destruction of letter boxes or mail—have no interstate commerce hook. Other crimes that have no interstate commerce hook include the following: sexually oriented advertisements (18 U.S.C. § 1735, 39 U.S.C. § 3010), explosive devices and nonmailable hazardous materials (18 U.S.C. § 1716), and firearms (18 U.S.C. § 1715). The U.S. Department of Justice (DOJ) joins the USPS in opposing the relaxation of the Mailbox Rule because these mail crimes do not include an interstate-jurisdictional hook (GAO, 1997; President's Commission on the United States Postal Service, 2003). Although most of these acts could be criminalized at the state level, if they have not been already (directly or indirectly),

it would be difficult to replace some federal provisions, such as the system regulating sexually oriented advertisements, particularly the list that the USPS maintains of addressees who have indicated a desire not to receive such advertisements and the administrative powers that the USPS can use against violators.

Similar to the discussion in the previous section, it is not clear what impact this loss of federal jurisdiction might have on public safety. Aside from the federal regulation of sexually oriented advertising, all or nearly all mail-crime statutes have a direct or indirect parallel on the state level. Every state has laws that would criminally penalize theft, fraud, stalking, murder for hire, child exploitation, and the use of weapons of mass destruction. As noted earlier, one argument is that local and state law enforcement agencies would not investigate lesser mail crimes. Although this argument may have some merit based on the experience of other countries, as noted in discussions with IS staff, U.S. Attorneys Offices will sometimes refuse to accept small mail crimes, forcing the IS to work with local law enforcement so that local district attorneys will prosecute the cases.

If Congress were to relax the Mailbox Rule, it would have several options for mitigating these jurisdictional issues somewhat. If the loss of federal jurisdiction over diverted deliveries is a concern, Congress could insert interstate commerce jurisdictional hooks into mail-crime statutes that currently rely only on the mail for federal jurisdiction, such as sending explosive devices, nonmailable hazardous materials, and firearms. Of course, this would not reach *intra*state crimes. The IS is correct in saying that diversion of mail to private couriers would take many types of crime out of federal jurisdiction.

If Congress is concerned that diversion from relaxing the Mailbox Rule will limit the public's benefit of having a specialized law enforcement agency, it could grant the IS investigative jurisdiction over mail crimes for mail diverted to private couriers (where federal jurisdiction can be established). However, the IS indicated in discussions that this would place it in the awkward position of regulating the USPS's competition, particularly if relaxation of the Mailbox Rule is intended to reduce the USPS's competitive advantage. (A monopoly beneficiary usually does not become the industry regulator when it loses its

monopoly.) The IS would likely have to be removed from the USPS to enable it to fairly regulate the USPS's competition. This would involve the logistical complexity of bureaucratic reorganization, as well as have cost implications. If the IS were not removed from the USPS but were still mandated to police the USPS's competition, one would anticipate that investigative costs (currently funded by taxpayers) would rise for cases involving private couriers because new relationships would need to be created and federal jurisdiction based on interstate commerce would have to be established in each case through a preliminary investigation.

Relaxing the Mailbox Rule: Effect on Investigation Costs

In addition to reducing the scope of the IS's investigative jurisdiction, another IS concern is that relaxing the Mailbox Rule would be deleterious to public safety because it would make IS criminal investigations more difficult and expensive, thus reducing its investigative efficiency.

Most obviously, even if mail retains its status as mail once delivered to a mailbox, relaxation of the Mailbox Rule would result in more people making deliveries to a mailbox. Even if a licensing regime were created that would limit mailbox access to agents of licensed courier services, or only the current large private courier companies, the number of people legally accessing a mailbox would increase. Hence, any investigation involving mailbox surveillance would have more potential suspects to eliminate.[3]

In addition, the IS is concerned that relaxing the Mailbox Rule will result in a number of calls for service about deliveries not involving mail. The USPS argues that it might not be obvious to all consumers that a delivery came from a private courier, particularly if couriers use their own form of stamps. More important, customers might not think to distinguish between deliveries from the USPS and private couriers

[3] This logic would apply somewhat less to rural households that private couriers reach using the USPS last mile service because there would be a smaller increase in the number of persons delivering to their mailboxes.

when reporting a delivery-related crime. This would expose the IS to the incremental costs of having to determine whether the delivery was mail each time it responds to complaints. If Congress granted the IS investigative authority over mail crimes for mail diverted to private couriers, the IS would have to determine whether a statute with an interstate commerce federal jurisdictional hook applies and whether an actual interstate commerce nexus exists in the potential case before opening a full investigation. (No exploratory investigation is necessary because, currently, mail crimes are always federal crimes.)

Changing the Mailbox Rule would likely affect the IS's investigative role. These changes would require additional training to prepare Postal Inspectors for working in a new environment. The IS's ability to coordinate communication, collect evidence, and organize investigations among multiple parties would change. It would have to create and maintain a broader network of relationships, among both couriers and local law enforcement agencies.

Some of these issues can be partially mitigated, such as by requiring private courier companies to clearly mark their deliveries. Even so, if the Mailbox Rule is relaxed, individual IS investigation costs would likely rise, particularly if the mailbox remains an authorized depository for mail. Without an increase in mailing prices or a federal appropriation offsetting the rise in costs, the IS would likely have to shift its resources according to new budgetary realities. Of course, these higher costs might be offset somewhat by a smaller caseload to the extent that relaxing the Mailbox Rule reduces the scope of the IS's investigative jurisdiction.

Relaxing the Mailbox Rule: Effect on Tracking Trends in Mail Crime

As noted in discussions with IS staff, another important concern is that the IS will lose visibility into mail crimes nationwide if the Mailbox Rule is relaxed. Currently, the IS receives and tracks most, if not all, mail-crime complaints nationwide. Other law enforcement agencies know to refer mail-crime reports to the IS. The IS can analyze this

information to identify trends, patterns, and hot spots across state and local jurisdictional lines to focus its investigative resources, its public-awareness efforts, and to provide advice to other law enforcement agencies (see Chapter Two). If the rule were relaxed, crimes that would lose their federal status because of diversion or the mailbox ceasing to be an authorized depository would no longer be properly reported to the IS. This would deny the public the safety benefits that come from the IS's and the DOJ's current ability to track mail-crime trends. As noted in our discussions with New Zealand Post, although New Zealand Post retained the largest market share under deregulation, it recognizes that it no longer has visibility into what incidents are occurring across the entire market.

One means of mitigating the loss of knowledge that would follow this loss of visibility would be for Congress to establish a mandatory mail crime–reporting system. The IS could be the clearinghouse for mail crimes, just as the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) is the clearinghouse for all firearm-related crimes. (By way of comparison, ATF is approximately the same size as the IS; see Lluberes, 2005.) This proposal would likely involve increased costs for the IS. If Congress makes the IS the clearinghouse for mail crimes, it should be a funded mandate. As noted in discussions with IS staff, another concern is that this would place the IS in the awkward position of regulating the USPS's competition. To avoid this problem, the burden of reporting could be placed on law enforcement agencies. Currently, agencies refer reports of mail crimes to the IS. Under this proposal, those agencies could continue to refer mail crimes to the IS and report crimes that the IS no longer investigates. The IS might also need to further expand its participation in interagency task forces to give technical assistance to local law enforcement in cases in which the IS has lost authority to investigate.

Relaxing the Mailbox Rule: Effect on the Ability to Deter Crime

A key IS concern is that relaxing the Mailbox Rule will reduce its deterrent effect against crime at the mailbox by ending the current regime under which only USPS employees and customers have legal authority to access the mailbox. (Note that everyone has legal authority to access a mailbox, as long as only mailable matter with proper postage is deposited.)

The primary reason for creating criminal laws and enforcing them is to deter people from performing certain acts. Generally speaking, deterrence theory holds that a person who is considering committing a crime will weigh the benefits of committing the crime against the costs of committing it. Chapter Three discussed an element of deterrence theory—limiting the ease of opportunity to commit a crime. An example of this type of deterrence is putting floodlights or cameras in an area where crime frequently occurs. In this section, we discuss two elements of deterrence that affect how the existence of a law and the enforcement of the law may influence individual criminal choices. The first element is the *normative* component of deterrence: Individuals should be aware that committing the crime is wrong because society has criminalized the behavior and punishes people for that behavior (e.g., mail theft is illegal so one *should not* steal mail). The second element is the basic element of the cost analysis: the likelihood of being caught and being punished.

Does Enforcement of the Mailbox Rule Deter the Acts It Proscribes?

Although ignorance of the law is never a defense in court, the normative component of deterrence requires that a person know not to perform a particular act.

The Mailbox Rule presents an interesting situation. It was intended to prevent private companies from making deliveries without postage to the mailbox. That almost no companies do so indicates that the statute succeeds in deterring this behavior. The IS and USPS handle the occasional violations that do occur administratively, collecting the amount of postage due without bringing criminal charges.

However, the Mailbox Rule is a criminal law that applies to the general population, not just utility companies or private courier companies. Whether the Mailbox Rule can have any deterrent effect on individuals considering committing other mail crimes requires that they be generally aware of the Mailbox Rule itself. It appears that much of the public is not aware of the Mailbox Rule. Mailable matter (such as an envelope holding keys) is frequently deposited or retrieved from unlocked mailboxes by family, friends, and acquaintances with a USPS customer's expressed or assumed permission. Although this study did not include this question in the survey discussed in the next chapter, one would assume that most people who perform such a benign activity likely do not realize that they are committing a federal crime. Hence, in this sense, the Mailbox Rule has questionable normative deterrent effect for the general public.

The Mailbox Rule cannot have any risk-based deterrent effect for the general public because arrests and prosecutions for violating the rule almost never occur. During its first 50 years, *no one* was prosecuted for violating it (*Greenburgh Civic Associations*, 453 U.S. at 155). A search of the database of lead charges in federal prosecutions created by Transactional Records Access Clearinghouse (TRAC) at Syracuse University reveals that, during the past 10 years, only *one* person has been prosecuted for its violation. The IS forwarded three other cases for prosecution, but U.S. Attorneys Offices declined to prosecute. Accordingly, there is clearly no risk to private individuals of being prosecuted for making the occasional delivery of mailable matter without postage to the mailbox.

U.S. Supreme Court Justice John Paul Stevens noted the Mailbox Rule's lack of deterrent effect for the general public in his dissent in *Greenburgh Civic Associations* in 1981:

> [W]e should not ignore the fact that nobody has ever been convicted of violating this middle-aged nationwide statute. It must have been violated literally millions of times. Apparently the threat of enforcement has enabled the Government to collect some postage from time to time or to cause a few violators to discontinue their unlawful practices, but I have the impression that the general public is at best only dimly aware of the law and the

> numerous otherwise law-abiding citizens regularly violate it with impunity. (453 U.S. at 155)

Does Enforcement Deter Crimes at the Mailbox?

When the IS discusses the Mailbox Rule's deterrent effect, it is not referring to violation of the Mailbox Rule itself but to its potential secondary effects to deter other mail crimes. This section analyzes the deterrent effect of mail-crime statutes prohibiting crimes at the mailbox—the crimes that might lose federal jurisdiction if the Mailbox Rule were relaxed and the USPS were to remove the mailbox's status as an authorized depository of mail matter. It considers both whether enforcement of the Mailbox Rule might play a role in deterrence of these other crimes and whether these other crimes have a deterrent effect that would be lost should the mailbox cease to be authorized depositories of mailable matter.

Normatively, even if individuals are not aware of federal statutes prohibiting mail theft, mail or mailbox destruction, or obstruction of mail, it is likely that they recognize that these acts are improper and probably illegal. This implies a normative effect to the crimes themselves, but it implies no deterrent effect from the Mailbox Rule.

If individuals who are considering committing a crime at the mailbox analyze the risk of getting caught, it is theoretically possible that the Mailbox Rule's implicit limitation on the number of people delivering to the mailbox might cause them to be surreptitious in committing their crimes. However, any criminal who hopes to avoid capture would attempt to be surreptitious, and the Mailbox Rule confers no threat of prosecution.

Looking at mail theft, the most common mailbox crime, it is evident that the federal proscription of mail theft has almost no risk-based deterrent effect that would be lost from canceling the mailbox's status as authorized depository. Approximately half to two-thirds of the IS's annual arrests are for mail theft. However, the number of arrests is minuscule in comparison to the number of complaints of mail theft that the IS receives annually. Using IS data provided to the GAO in FY 1996, the IS arrested 4,777 persons (including 499 USPS workers) for mail theft, but it received *more than 2.4 million* complaints

of mail theft that year (GAO, 1997, p. 27).[4] In other words, less than 0.2 percent of mail-theft complaints result in arrest. This suggests that enforcement of the mail-theft statute has minimal risk-deterrence effect, at least for small-time mail thieves.

Of course, many mail theft arrests are for volume attacks. The IS concentrates its limited resources on large-scale mail theft, with good results: The IS reports that volume attacks fell by 35.7 percent between FY 2006 and FY 2007 (IS, 2008c, pp. 17–18). The IS has succeeded in breaking up mail-theft rings in some cities, reducing large-scale mail theft significantly. For instance, the IS worked with federal and local law enforcement agencies in Denver to close down a large mail-theft and check-fraud ring, reducing monthly volume mail attacks in the Denver area from 40 in December 2005 to only two in May 2006 (IS, 2007a, p. 21). Even so, if volume attacks account for many mail theft complaints, each arrest would have to account for an average of 502 complaints for the 4,777 people arrested to account for the 2.4 million complaints. In addition, the IS sometimes works with state or local law enforcement to effect arrests when a U.S. Attorneys Office refuses to prosecute small crimes.

Hence, if crimes at the mailbox are no longer subject to IS investigation because of relaxing the Mailbox Rule, the IS would lose its ability to deter large-scale mail-theft rings through its focused policing efforts. Conversely, small-time mail thieves may still be arrested by state or local law enforcement.

Do the USPS and IS Deter Crimes That Might Be Diverted to Private Couriers?

As discussed, relaxing the Mailbox Rule would result in some diversion of mail to private couriers. Here, we focus on the risk analysis of people considering committing a mail crime: Would they believe that they would run a lower risk of getting caught if they used private couriers instead of the USPS? This involves two risk analyses: (1) the risk of

[4] Although the specific breakdown of these complaints is not clear, the IS stated that "it is safe to characterize a large and significant portion of this number as theft from mailboxes" (GAO, 1997, p. 27).

detection by private couriers and (2) the risk of punitive consequences from law enforcement.

There are minimal data to analyze the comparative risk of detection between private courier companies and the USPS. As discussed in Chapter Three, there is some evidence that the USPS is more vigilant in detecting suspicious or hazardous items before delivery. If the Mailbox Rule were relaxed such that couriers beyond the major current companies could enter the market, one might surmise that some couriers might not be able to equal the USPS and the major courier companies in terms of training, detection technology, policies, and procedures. If the risk of detection by some courier companies is deemed to be lower, this would present a particular concern about crimes in which both the sender *and* the recipient hope to avoid detection, such as in the distribution of child pornography. It would also present a concern in cases in which the sender is duped and the recipient hopes to evade detection, such as fraudulent applications for checks or credit cards. Of course, this remains guesswork.

The risk of punitive consequences from law enforcement has already been discussed with regard to such crimes as mail theft; the risk is low. In comparison, more-spectacular crimes, such as sending or directly delivering bombs to the mailbox, are guaranteed investigation by law enforcement—local, state, or federal (or perhaps a combination thereof). While state law may not criminalize sending a bomb by mail or courier per se, such an act would almost certainly qualify for prosecution as assault, battery, (attempted) manslaughter, or (attempted) murder.

However, some federal mail laws may have no state parallel. It is possible that some states will not prohibit some acts that are criminalized by federal law, allowing criminals to use private couriers on an intrastate basis to avoid federal penalties. In addition, the IS has administrative powers to stop or seize mail in situations that inspectors determine do not rise to the level of requiring criminal sanctions. Among its powers to stop mail under 39 U.S.C. §§ 3001–3010 is the federal regulation of sexually oriented advertisements (39 U.S.C. § 3008). The USPS maintains a list of addresses that indicate they wish to receive no such advertisements; senders are penalized for violating the rules.

Summary

This chapter's analysis finds that relaxing the Mailbox Rule would likely reduce the number of crimes that the IS could investigate. Relaxing the Mailbox Rule would also challenge the IS's ability to police the mail crimes remaining in its jurisdiction.

In discussions with IS staff, one assertion is that logistical concerns will cause the USPS to treat the mailbox like mail slots if the Mailbox Rule is relaxed. While USPS and IS operating costs are likely to rise as a result of relaxing the Mailbox Rule, canceling the mailbox's status as an authorized depository of mail is not inevitable. Congress could mandate that the mailbox remain an authorized depository of mail to maintain federal jurisdiction over U.S. mail in the mailbox and perhaps over mailboxes themselves, but the IS would face a strain on its resources unless its higher costs were offset.

The IS is correct to argue that deliveries that are diverted to private courier companies will not be covered by federal mail-crime statutes unless the statute provides an interstate commerce federal jurisdictional hook and an actual interstate commerce nexus exists in the case. This problem could be mitigated somewhat by increasing the number of statutes with a federal jurisdictional hook. However, this would not cover *intra*state crimes.

The IS is also correct to argue that it will not have investigative jurisdiction over deliveries diverted to private courier companies, even those with interstate commerce–based federal jurisdiction. If Congress chose to relax the Mailbox Rule but wanted to apply the IS's policing capabilities to diverted mail, it would place the IS in the awkward position of regulating the USPS's competition.

Relaxing the Mailbox Rule also would reduce the IS's ability to effectively police mail crimes that remain in its jurisdiction because the cost and complexity of investigations would likely rise and its visibility into national mail-crime trends would be reduced by a shrinkage in the amount and consistency of information. The reduction in the IS's caseload might offset some of the cost increases created by relaxing the Mailbox Rule. The latter problem could be mitigated if Congress instituted a mandatory reporting system.

Finally, the impact that relaxing the Mailbox Rule would have on deterrence of crime is likely overstated. In our view, at present, the only evident deterrent effect that might be reduced would be if the mailbox were treated as a mail slot and the IS were unable to continue its strategic focus on large-scale mail thefts.

CHAPTER FIVE

Public Perceptions About Relaxing the Mailbox Rule

When it comes to current restrictions on mailbox access, one argument is that it provides USPS customers with the assurance that their mail is secure and that their correspondence will not become known to third parties. Further, the current restrictions facilitate the investigation of mail theft and other mail crimes by having a designated federal entity responsible for doing so. Opening up access to the mailbox may increase the volume of unsolicited advertising mail and other mail at the point of delivery, will increase the number of individuals who have legal access to one's mailbox, and raises a number of questions about who is responsible for investigating mail crime.

Public opinion is important to the USPS, an independent establishment of the executive branch of the U.S. government, which has responsibility not only to its customers as a business but also to the public as a whole. Limited research has been conducted on what the public thinks about the Mailbox Rule and about any proposals to open up access to the mailbox, as well as about public perceptions of how secure the mail is and the USPS's role in this regard. Two previous surveys (discussed below) identified a positive perception of the USPS and public opposition to opening up access to the mailbox. However, the reasons for that opposition and the extent to which security played a part in them are unclear. Further, one of those studies was conducted prior to the 9/11 terrorist and anthrax attacks, when the public had a less heightened concern about security, and the other study was conducted in 2003, several years after the terrorist attacks. Our interest

was in seeing how public opinion may have changed, if at all, now that we have some distance from 9/11.

To obtain more current data on the public's perceptions and on reasons underlying decisions to favor or oppose opening up access to private companies and individuals, we undertook a survey of consumers as part of the RAND Corporation American Life Panel (ALP), an established panel weighted to be representative of the nation as a whole.[1] In this chapter, we begin with a brief summary of the methods used to examine public concerns, followed by a summary of the key findings and conclusions.

Methods

We initially conducted a literature review on public perceptions of the Mailbox Rule and of USPS service generally. We identified two main studies that examined public perceptions of the Mailbox Rule—a U.S. Government Accountability Office (GAO; then, the U.S. General Accounting Office) (1997) report and a survey from Peter D. Hart Research Associates (2003) on behalf of the President's Commission on the United States Postal Service. The GAO conducted a survey with 1,013 households in 1996 as part of its report *U.S. Postal Service: Information About Restrictions on Mailbox Access* (GAO, 1997); that survey focused on the Mailbox Rule. Peter D. Hart Research Associates completed surveys of 760 respondents on May 19 and 20, 2003, with a range of questions about possible improvements of the USPS system, including two questions about the Mailbox Rule. We also solicited and received some internal USPS market research on the issue, drawn from a survey of 2,021 individuals conducted by Opinion Research Corporation.

None of the surveys examined reasons for opposing or supporting opening up access to the mailbox. Therefore, we developed our own

[1] Consistent with the previous surveys, we focus on private consumers, rather than corporate or institutional consumers who may have different concerns in light of different methods of delivery (potentially greater interaction with courier services) and content of items received (potentially at greater risk of receiving hazardous or suspicious items).

interview survey using the ALP, an ongoing panel survey maintained by the RAND Corporation that consists of approximately 1,500 respondents. The panel was originally recruited from respondents age 40 years and older in the Monthly Survey of the Survey Research Center at the University of Michigan, but it has subsequently been supplemented with younger respondents to make it representative of the U.S. population age 16 years and older.[2] Having been selected, these respondents are sent survey questionnaires on a variety of topics several times per month, to which they respond via the Internet to facilitate high response rates in a short period. The majority of the panel members (about 1,250) had their own Internet access before being selected for the ALP (ALP, 2005). RAND provided free Internet access through WebTV to the remaining panel members. This eliminates the bias in sample selection found in many Internet survey panels, which include only computer owners.[3]

Our questionnaire was designed to maintain consistency with the previous surveys and then delve into the reasons behind the responses. We developed questions similar to the GAO survey, the Hart survey, and the USPS internal research to be able to examine opinion changes over time. The sample was split into halves for the initial question, with one half getting a question on mailbox access nearly identical to that in the GAO survey and the other getting a question on mailbox access similar to that in USPS internal research. The goal was to examine whether having more information about relaxing the Mailbox Rule would change one's opinion and reasons for opposing or supporting such a proposal. This was followed by questions about reasons for supporting or opposing opening up mailbox access, perceptions about mail security, and demographic information specific to mail usage. The questionnaire can be found in Appendix A.

---

[2] The Monthly Survey is the leading consumer-sentiment survey that incorporates the long-standing Survey of Consumer Attitudes and produces, among others, the widely used Index of Consumer Expectations.

[3] Excluding individuals without Internet access would likely bias the sample, because these individuals differ significantly both socioeconomically and geographically from those with Internet access. Providing Internet access to the ALP sample ensures that these individuals are not excluded.

Analysis of the data included cross-tabulation and statistical tests for significance. The data were weighted to be nationally representative, using post-stratification weights provided by ALP. Demographic data were also incorporated. ALP respondents provided some of the demographic data directly, including information on gender, age, income, race, and location. These location identifiers were linked with data from the U.S. Census Bureau to assign neighborhood status as rural or urban, as defined in Chapter Three.

The final sample that we use for estimation consists of 1,314 respondents interviewed in July 2008 (88-percent response rate). The sample contained 49 percent men and 51 percent women.[4] The mean age of the sample was 44.8 years. Family income was calculated categorically, with a median family income between $40,000 and $49,000. The sample was 84 percent white (including Hispanic), with 10 percent black or African American, 2 percent American Indian or Alaskan, and 2 percent Asian or Pacific Islander. Finally, the sample was 19 percent rural and 81 percent urban.

Key Survey Findings

Most Respondents Have a Positive Perception of the USPS

Using a format similar to what has been used in USPS market research, the ALP survey asked individuals how they perceive the USPS. Respondents had a positive perception of the USPS, seeing the USPS as reliable (89 percent of respondents agreed or strongly agreed), secure (77 percent), private (70 percent), and convenient (88 percent) (Table 5.1). These results are consistent with the USPS's own market research (USPS, undated[c]). Additionally, two other surveys of note support our results of positive perceptions in the specific areas of privacy and security, and three other surveys support our findings of a positive perception generally.

Most important for our purposes was the perception of security: We found that 77 percent of the respondents agreed or strongly agreed

[4] Weighted sample characteristics are presented.

Table 5.1
Perceptions of the USPS Brand (%)

Would you say your mail service is . . .	RAND ALP Survey (1,314 respondents)						USPS Survey
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Don't Know	Agree
Reliable?	36	53	6	4	1	0	92
Secure?	24	53	15	6	1	4	79
Private?	22	48	21	7	2	1	82
Convenient?	42	46	8	3	1	0	92

with the statement that the USPS is secure (as shown in the shaded row of Table 5.1). This is consistent with a 2001 Gallup survey (Moore, 2001) that asked about approval of how various government agencies were handling the war on terrorism, with a specific mention of the USPS. The survey, taken in November 2001, found that 77 percent of Americans approved of the way the USPS was handling the war on terrorism (Moore, 2001). As time passes since the anthrax attacks of 2001, it is unclear whether those perceptions have remained stable with regard to the USPS. However, general support for governmental efforts to protect the United States from terrorism have remained stable: In August 2006, 73 percent of respondents had a great deal or fair amount of confidence in the U.S. government to protect its citizens, as compared to 76 percent in May 2002 (Moore, 2001). During that same period, concern about terrorism has increased only slightly since the spike in concern immediately after 9/11.

We also found that 70 percent of respondents felt that their mail service was private. This is consistent with related surveys from the Ponemon Institute. The Ponemon Institute annually surveys individuals' trust in government agencies to safeguard personal information (see, e.g., Ponemon Institute, 2008). In 2008, the Ponemon Institute reported that 86 percent of the public trusts the USPS, one of the oldest government agencies in the United States, and that the USPS has increased that level of trust every year. According to the 2007 Privacy

Trust Rankings, the American public has rated the USPS as the most trusted government agency for four years in a row (USPS, 2008a).

Three additional studies support our finding of a positive perception of the USPS generally. The 1996 GAO (1997, question M1) survey found that 91 percent of respondents were satisfied or very satisfied with the USPS. The Hart Research Associates survey in May 2003 found that 79 percent of people had a positive or very positive perception of the USPS, while only 9 percent viewed the USPS negatively (Hart, 2003, question 1). Hart also referenced an earlier survey that found that the positive perception of the USPS had increased since earlier surveys in 2001 and 1994. It is worth noting, however, that the Hart survey also found an almost identical positive perception for UPS (78 percent positive, 4 percent negative, with 7 percent saying that they were unsure or did not know) and FedEx (71 percent positive, 3 percent negative, with 14 percent saying that they were unsure or did not know). Finally, a GfK Roper survey in August–September 2007 found the USPS to be the most popular agency in the government, with an 81-percent favorable rating (Carlstrom, 2008).

Most Respondents Oppose Removing the Mailbox Rule

The ALP survey was intended to gather data on reasons for opposing or supporting removal of the Mailbox Rule—information not gathered in previous surveys. In addition, we assessed whether having more or less information about removal of the Mailbox Rule would influence individuals' responses. As noted earlier, our survey split the sample into two parts; half of those surveyed were asked a question similar to that in the GAO survey, and the other half was asked a different question that provided more detail about the Mailbox Rule, which was consistent with previous marketing surveys by the USPS. The difference was intended both to examine whether more information might affect how respondents viewed the proposed relaxation of the Mailbox Rule and to provide comparability to prior data.

For the ALP survey, in the first version of question 1 (the GAO version), individuals were asked who should be allowed to leave mail in their mailboxes (exact wording of the question can be found in Table 5.2, as well as in Appendix A). A majority of respondents

Table 5.2
Preference for Access to the Mailbox: GAO Version

Question 1.1. Only the US Postal Service is currently allowed to leave mail in your mailbox. Some people say that it should stay that way. Other people say that some companies should also be allowed to put mail inside mailboxes. Which of these statements comes closest to your view?	Overall (%)
U.S. Postal Service Only	55
Some parcel companies such as FedEx or DHL should also be allowed	33
Other companies (e.g., local hand delivery firms) should also be allowed	5
Any individual should be allowed	5
Not sure/don't know	2

NOTE: Number of respondents = 607.

preferred that only the USPS have mailbox access, with one-third desiring that access be extended to large parcel companies, such as FedEx or UPS as well. Very few individuals were interested in other companies or individuals being given legal access.

These results were consistent with the opposition to opening up mailbox access found in the 1996 GAO (1997) survey. Individuals were asked about their opinion of opening up mailbox access, with 61 percent wanting mail to be delivered by the USPS only. An additional 32 percent of GAO-survey respondents wanted access opened up only to some additional companies (GAO, 1997, question M5). This suggests that the preference for USPS-only access has remained constant for more than a decade.

The decreasing support—from trusted parcel companies to other companies to any individual—is also consistent with the GAO survey. The GAO survey probed about the kinds of companies that should be given access to the mailbox. A majority supported FedEx or UPS having access (58 percent favor or strongly favor), and 48 percent supported allowing utility companies to have access (48 percent strongly favor or favor) (GAO, 1997, question M4). However, they disapproved of extending mailbox access more broadly: General or strong opposition to direct access was 54 percent for magazines and newspapers;

66 percent were opposed for catalogs, coupons, or ad mail; and 82 percent were opposed to giving individuals access to the mailbox.

For the ALP survey, in the second version of question 1 (the USPS version), individuals were given extensive information about the Mailbox Rule and asked whether individuals approved or disapproved of this exclusive access (exact wording of the question can be found in Table 5.3, as well as in Appendix A).

A majority of the respondents (66 percent) approved of the USPS having exclusive access to the mailbox (Table 5.3). However, these results should be interpreted with caution. From the comments received, as well as from the analysis of the data, it is clear that some respondents had difficulty in interpreting what was meant by "having exclusive access." This confusion was reflected in the responses.

Table 5.3
Preference for Access to the Mailbox: USPS Version

Question 1.2. As you may know, the Postal Service has the exclusive right to deliver U.S. mail. The Postal Service letter carrier delivers mail into the mailbox, for some customers through the door slot, and may retrieve mail placed in the mailbox by the customer for collection. No other individual, organization, or entity is legally permitted to insert materials into or extract materials from the mailbox. Some groups are suggesting opening access to mailboxes. Opening access to your mailbox to others, in addition to the U.S. Postal Service, would provide the convenience of allowing individuals and organizations desiring to contact, solicit, or provide information to you to insert information directly into your mailbox. The Postal Service would continue to deliver U.S. Mail into the same mailbox. Although the federal laws that protect the U.S. Mail would not apply to the items placed in the mailbox by others, state laws may provide protection. Do you approve or disapprove of having exclusive access to mailboxes? Would you say you . . .	**Overall (%)**
Strongly approve?	53
Approve?	13
Neither approve nor disapprove?	7
Disapprove?	12
Strongly disapprove?	13
Not sure/don't know?	3

NOTE: Number of respondents = 708.

A quarter of respondents who strongly disapproved of the USPS having exclusive access to the mailbox, in a subsequent question, also did not support private companies having access (question 2).

In the ALP survey, using the USPS version of question 1, our finding of a preference for exclusive USPS access was similar to that of the Hart survey. The Hart survey's respondents were asked whether they supported or opposed removing the Mailbox Rule. Seventy-one percent strongly opposed or opposed doing so; however, the Hart survey (2003, question 13b) prefaced the question with a presumption that there would be an increased amount of ad mail, which may have influenced the responses.

This opposition may not be as homogeneous as it initially appears. While opposition to opening up access has remained constant for at least the past 15 years, so has actual postal access. However, individuals who receive their mail through a door slot are subject to different rules about mailbox access. As noted in Chapter Four, mail slots are not afforded the same protections as the mailbox itself. In some ways, their situation is akin to having no Mailbox Rule, as any individual can approach a house with a door slot and deliver mail directly. However, in other ways, it is not akin to a removal of the Mailbox Rule, in that already delivered mail is less accessible for mail theft. Respondents who get their mail through a slot in the door are generally more in favor of expanding mailbox access under either version of question 1 (GAO or USPS version). This may reflect an overall lower risk of mail theft in their situation or it may reflect a bias toward the status quo.

Respondents with door slots who were asked the GAO version of question 1 were most likely to prefer some parcel companies having access, while USPS exclusive access was preferred by only about 29 percent of the sample, as compared to being preferred by about 55 percent of all respondents (Table 5.4).[5] The difference in mean response between those with a door slot and those with other types of receptacles was statistically significant at the $\alpha = 0.05$ level.[6] Individuals with

[5] Individuals with door slots comprised 4 percent of the sample.

[6] All tests of significant differences included controls on gender, family income, being nonwhite, and rural residence (where applicable).

Table 5.4
Preferences for Mailbox Access for Those Who Receive Mail Through a Door Slot

	Question 1.1 (GAO Version) [mailbox access]			Question 1.2 (USPS Version) [exclusive access]	
Response	**Overall (%)**	**A slot in the door (%)**	**Response**	**Overall (%)**	**A slot in the door (%)**
U.S. Postal Service Only	55	29	Strongly approve	53	31
Some parcel companies	33	37	Approve	13	36
Other companies	5	31	Neither approve nor disapprove	7	5
Any individual	5	0	Disapprove	12	7
Not sure/don't know	2	3	Strongly disapprove	13	12
			Not sure/don't know	3	10
Number of respondents	607		Number of respondents	708	

door slots who were asked the USPS version of question 1 were more likely to approve rather than strongly approve, as the overall sample preferred, but this result is only suggestive rather than statistically significant, and overall approval was the same for those with and without door slots.

Overall, we found that individuals do not support changing the Mailbox Rule to open up access to other couriers. These perceptions have remained consistent over time. The public's resistance to opening up access is similar to that found in the GAO (1997) survey and the Hart (2003) survey. Further, although most individuals do not support ending the Mailbox Rule, they may be open to trusted companies and known delivery companies having access.

Security Is One Concern Among Many

Past examinations of the reasons that people oppose opening up access to the mailbox have not fully answered the question about reasons for doing so. In an open-ended, qualitative statement with no aggregate results being publicly released, the GAO (1997) survey asked why respondents opposed increased access. The Hart survey asked respondents why they opposed greater access, but it prefaced the question with an assumption that there would be greater amounts of ad mail. Although that presumption did not seem to affect the opposition to opening up access, it raises the concern that it may have affected the stated reasons for that opposition.

We asked the ALP sample what it believed was the strongest reason for opposing increased access, with most respondents citing security-related reasons. Forty percent felt that opening up access would make the mail less secure, followed by concerns that it may lead to identity theft (21 percent) or make the home less secure (10 percent) (Table 5.5). Concerns about junk mail were the largest non–security-related response (15 percent), but increases in cost were similarly concerning. Our findings suggest that security is a larger concern than previous surveys showed.

We also found a correlation between perceived risk (both at the mailbox and in the processing of mail) and opposition to opening up mailbox access. The more concerned individuals were about security, the

Table 5.5
Reasons to Oppose Increased Access

Question 3. Which one of the following would you say would be the strongest reason for opposing a proposal to allow private companies to compete for the opportunity to deliver mail to your home mailbox?	Overall (%)
Make home less secure	10
Could lead to identity theft	21
Make mail less secure	40
Would be more expensive	15
Would lead to more "junk mail"	15
Other reason	2
Not sure/don't know	5
Don't oppose	2

NOTE: Number of respondents = 1,314.

more likely they were to want to restrict access to their mailboxes. This was true for both versions of question 1 (GAO and USPS) on mailbox access (Tables 5.6 and 5.7).

Table 5.6
Perceptions of Mailbox Access, by Level of Concern About Mailbox Security

		By security concern (%)			
Question 1.1 (GAO version) [mailbox access]	Overall (%)	Very concerned	Somewhat concerned	Not very concerned	Not at all concerned
U.S. Postal Service Only	55	77	58	57	39
Some parcel companies . . .	33	14	38	31	39
Other companies . . .	5	3	2	5	5
Any individual . . .	5	5	1	5	12
Not sure/don't know	2	2	1	2	4

NOTE: Number of respondents = 607.

Table 5.7
Perceptions of Mailbox Exclusivity, by Level of Concern About Mailbox Security

Question 1.2 (USPS version) [exclusive access]	Overall (%)	By security concern (%)			
		Very concerned	Somewhat concerned	Not very concerned	Not at all concerned
Strongly approve	53	61	51	57	40
Approve	13	20	17	11	7
Neither approve nor disapprove	7	9	5	9	8
Disapprove	12	0	11	13	19
Strongly disapprove	13	8	13	10	26
Not sure/don't know	3	2	3	1	1

NOTE: Number of respondents = 708.

Overall, we found that 77 percent of respondents were concerned that opening up mailbox access to private companies would increase security risk. This finding is consistent regardless of the version of the question given (Table 5.8). Respondents who were given more information about opening up mailbox access (USPS version of question 1) were more concerned (83 percent) about increased private access than were those (71 percent) who were given the GAO version. This difference was statistically significant at the $\alpha = 0.05$ level. Because a large majority of respondents believed that opening up mailbox access to private companies would increase security risk, it is intuitive that those who are most concerned about security would also be most opposed to increased access.

Further examination of the ALP data supports this finding. Not only are greater concerns about crime in mail processing correlated with a desire to maintain exclusive USPS access, but higher perceptions of USPS security and beliefs that private companies would increase security risks were all correlated with a desire to maintain mailbox access as well.

Table 5.8
Increasing Access to Private Companies Increases Concerns About Security

Question 8 (how level of concern about security breaches/crime would change if other companies were allowed to sort, process, and transport mail)	Overall (%)	Question 1.1 (GAO version) (%)	Question 1.2 (USPS version) (%)
More concerned	77	71	83
Would not change	17	22	13
Less concerned	3	4	2
Don't use the mail	0	0	1
Not sure/don't know	2	4	1
Number of respondents	1,314	607	708

The ALP respondents were also asked how concerned they were about mailbox security and about security breaches in mail processing, sorting, and delivery. Fifty-eight percent were not at all concerned or not very concerned about mailbox security, and 53 percent were not at all concerned or not very concerned about security breaches or crimes committed in mail sorting, processing, or transporting (Table 5.9). This result is not unexpected given that close to 80 percent of respondents reported earlier the belief that their mail overall was secure (see Table 5.1). That said, Table 5.9 indicates that increasing mailbox access would be associated with increased concern for the majority of individuals.

Additionally, a substantial minority of respondents who stated that opening up mailbox access to private companies would increase their security concerns still wanted to increase access to some parcel companies (29 percent) (Table 5.10). Of those who did not think that opening up access would increase security risk or that it would decrease risk, respondents were more likely to cite increased junk mail or higher costs rather than security concerns as the strongest reason to keep the Mailbox Rule. Additionally, concerns of delivery cost and speed were also cited as reasons to increase access (not shown). While security was an important concern, it was not determinative for all individuals.

Table 5.9
Concern About Security of the Mailbox and Mail Security (%)

Questions 6 and 7	At present, how concerned are you about the security of your mailbox?	At present, how concerned are you about security breaches or crimes committed in the sorting, processing, and transporting of mail?
Very concerned	10	10
Somewhat concerned	31	36
Not very concerned	41	40
Not at all concerned	17	13
Don't use a mailbox	2	0
Not sure/don't know	0	1

NOTE: Number of respondents = 1,314.

Table 5.10
Perceptions of Mailbox Access, by View of the Security Impact of Increasing Access

	Perceptions of mailbox access for individuals for whom . . .		
Question 1.1 [mailbox access]	Open access increased security concerns (%)	Open access did not change security concerns (%)	Open access decreases security concerns (%)
U.S. Postal Service Only	62	35	40
Some parcel companies . . .	29	44	43
Other companies . . .	4	10	7
Any individual . . .	4	9	5
Not sure/don't know	2	2	5

NOTE: Number of respondents = 607.

The data also suggest that the stated reasons for concern depended somewhat on how the questions were worded. The most obvious example of this comes from comparing our ALP survey results with the 2003 Hart survey results. While both surveys had similar responses

about whether mailbox access should be opened up, the reasons for opposing it were very different. The Hart survey had a similar proportion of respondents citing identity theft and a greater number of respondents citing home security, but mail security itself was not an option. The Hart survey question about reasons for opposing increased mailbox access primed the respondents with a presumption of additional ad mail, and respondents largely cited concerns about junk mail. We deliberately avoided such wording to examine opinions without altering their preconceptions, and, instead, we allowed more categories for expressing security concerns. Accordingly, the Hart survey largely cited concern about junk mail, while our ALP survey largely cited security concerns (Table 5.11).

Even if we were to ascribe all the other reasons in the Hart survey to mail security, it would still not account for the difference in responses. People's concerns may have changed in the past few years, but other surveys indicate that this is not the case. Gallup surveys show that there has not been an increase in concern about security since 2003, but rather a slight decrease (Moore, 2001). Additionally, similarities in other questions in both the ALP and Hart surveys suggest that there

Table 5.11
Reasons for Opposing Access: Difference Between ALP and Hart Surveys

Reasons for Opposing Increased Access	ALP Survey [Question 3] (%)	Hart Survey (%)
Make home less secure	10	17
Could lead to identity theft	21	19
Make mail less secure	40	—
Would be more expensive	15	—
Would lead to more "junk mail"	15	47
Other reason	2	15
Not sure/don't know	5	2
Don't oppose	2	—
Number of respondents	1,314	540

were not significant shifts in opinion in that interval. We ascribe the difference in responses to the differences in the wording of the questions, particularly the description of the protections associated with the Mailbox Rule. Respondents' opposition to increased access is uniform across differently worded questions, but wording likely affects the reasons given for those responses.

We find additional evidence for this pliability in our survey itself. As mentioned, the sample was split in two, with two versions of question 1 asking about the Mailbox Rule. Of the two, the USPS version of question 1 was more descriptive of the security concerns. Comparing responses from the two versions, those respondents who received the more descriptive version of question 1 were more likely to cite security concerns as reasons for opposing mailbox access.[7] The size of these internal differences was not as pronounced as the differences between the ALP and Hart surveys, but the difference in wording was also smaller (Table 5.12).

Table 5.12
More Security Information Leads to Greater Citations of Security

Reasons for Opposing Increased Access	Version 1 [less description of security] (%)	Version 2 [more description of security] (%)
Make home less secure	9	12
Could lead to identity theft	19	23
Make mail less secure	26	33
Would be more expensive	17	12
Would lead to more "junk mail"	17	14
Other reason	4	1
Not sure/don't know	5	4
Don't oppose	3	1
Number of respondents	607	708

[7] This was statistically significant at $p < 0.001$.

Households More Likely to Be Affected Are Less Opposed

Chapter Three detailed how rural households are less likely to be affected by opening up mailbox access than are urban households. We also found differences in public opinion between rural and urban areas. Urban respondents, who are more likely to be affected by opening up mailbox access, were also less opposed to it. While urban respondents still largely oppose increased mailbox access, their opposition is weaker than that of rural respondents.

We examined the results of the survey comparing respondents living in ZIP Codes where 50 percent or more of the population was defined as rural in the 2000 census with those in ZIP Codes that were less than 50 percent rural. While this does not fully describe the diversity of American neighborhoods, it does present a clear first level of examination.

Under both versions of question 1, rural respondents were more opposed to increased mailbox access (Table 5.13). For example, using the GAO version of question 1, 67 percent of rural respondents and 52 percent of urban respondents wanted only the USPS to have access to the mailbox. The public opposition to increased access was somewhat stronger among respondents living in rural areas; respondents living in urban areas were less opposed. Although the difference was not overwhelming, both rural and urban respondents still largely opposed increased access.

The reasons to support or oppose increased access are largely similar between the two groups (Table 5.14). Rural and urban respondents continue to cite mail security, identity theft, and home security, as well as expense and junk mail in similar proportions.

This difference in opposition is also not the result of differences in the perception of the USPS (Table 5.15). Perceptions of the USPS are largely similar between the two groups; for privacy and convenience, rural respondents view the USPS as marginally worse but view it as marginally more reliable. Perhaps, most important for this monograph,

Table 5.13
Rural and Urban Views of Mailbox Access

	Question 1.1 (GAO version) [mailbox access]			Question 1.2 (USPS version) [exclusive access]	
Response	**Rural (%)**	**Urban (%)**	**Response**	**Rural (%)**	**Urban (%)**
U.S. Postal Service Only	67	52	Strongly approve	58	51
Some parcel companies . . .	20	36	Approve	12	13
Other companies . . .	6	5	Neither approve nor disapprove	8	7
Any individual . . .	6	5	Disapprove	4	13
Not sure/don't know	1	2	Strongly disapprove	15	13
			Not sure/don't know	2	3
Number of respondents	105	501	Number of respondents	141	567

Table 5.14
Rural and Urban Reasons for Opposing Increased Access

Reasons for Opposing Increased Access	Rural (%)	Urban (%)
Make home less secure	13	10
Could lead to identity theft	22	21
Make mail less secure	28	30
Would be more expensive	12	15
Would lead to more "junk mail"	16	15
Other reason	2	2
Not sure/don't know	3	5
Don't oppose	4	1
Number of respondents	246	1,068

Table 5.15
Rural and Urban Perceptions of the USPS

Question 10 [USPS is . . .]	Reliable (%)		Secure (%)		Private (%)		Convenient (%)	
	Rural	Urban	Rural	Urban	Rural	Urban	Rural	Urban
Strongly agree	42	35	24	24	17	23	39	42
Agree	46	55	50	54	51	47	45	46
Neither agree nor disagree	5	6	17	15	17	21	10	7
Disagree	7	4	8	5	9	7	6	2
Strongly disagree	0	1	1	1	5	1	0	1
Don't know	0	0	0	0	0	1	0	0

NOTE: Number of rural respondents = 246. Number of urban respondents = 1,068.

there is no significant difference in perception of the USPS with regard to security.

However, there are two important differences between rural and urban households. First, rural respondents are more concerned with security both at the mailbox and in mail processing, handling, and delivery (Table 5.16). This difference between rural and urban respondents was statistically significant at the $\alpha = 0.05$ level.

Second, rural households may have more concern about the security of private companies (Table 5.17). The data are suggestive that rural respondents may be more likely to associate increased mailbox access by private companies with an increased concern about security. Rural

Table 5.16
Rural and Urban Perceptions of Mailbox and Mail Security

	Question 6 [mailbox security]		Question 7 [mail security]	
Response	**Rural (%)**	**Urban (%)**	**Rural (%)**	**Urban (%)**
Very concerned	11	9	12	10
Somewhat concerned	36	29	44	35
Not very concerned	36	42	34	41
Not at all concerned	15	17	9	13
Don't use a mailbox	1	2	0	0
Not sure/don't know	0	1	1	1

NOTE: Number of rural respondents = 246. Number of urban respondents = 1,068.

Table 5.17
Rural and Urban Perceptions of Security with Increased Private Access

Question 8 [change in concern with increased private access]	Rural (%)	Urban (%)
More concerned	81	76
Would not change	13	18
Less concerned	2	4
Don't use the mail	0	0
Not sure/don't know	4	2
Number of respondents	246	1,068

respondents are marginally more likely to say that they would be more concerned, but the difference was not statistically significant.

Summary

Overall, a majority of respondents preferred that only the USPS have mailbox access, although a third were in favor of extending access to the major parcel companies and known delivery companies. These results are consistent with previous studies suggesting that the opposition to opening up mailbox access has remained consistent for at least the past 15 years.

However, opposition to removing or relaxing the Mailbox Rule may not be as homogeneous as it initially appears. Individuals who receive their mail through a door slot are subject to different rules about mailbox access from those who use the mailbox. Individuals who receive their mail through door slots (rather than mailbox receptacles) are not subject to the Mailbox Rule. They were generally more in favor of expanding mailbox access than those with receptacles.

We also examined the reasons for opposing opening up mailbox access. We found that security considerations were cited as important in the support for the USPS and in public opposition for opening up access. Most respondents cited security-related concerns as their strongest reasons for opposing increased access. In general, the more concerned individuals were about security, the more likely they were to favor restricting access to their mailboxes.

Finally, both urban and rural respondents, in general, oppose opening up access. However, there is some evidence that opening up mailbox access is more acceptable to urban residents, those who will be most affected by it. Rural households are less likely to be affected by removing the Mailbox Rule; we found that rural households were more likely to oppose removing the rule. Urban households still oppose increased access, but there is a substantial minority that is in favor of increased access for known and trusted parcel companies.

To some extent, this difference may come from being more familiar with private couriers. As discussed earlier in this monograph, the

USPS has regular interaction with the public, contributing to a sense of familiarity and comfort. This is true for all households, urban and rural. However, rural households may be less likely to interact with private parcel companies on a regular basis than urban households are (through less frequent courier deliveries to rural areas or through the last mile USPS delivery of some courier-service items). This could contribute to a greater familiarity for urban respondents than rural respondents, alleviating urban concerns over private parcel companies. If access were granted to private parcel companies, it is unclear whether public opinion may shift as individuals became more familiar and comfortable with these companies.

CHAPTER SIX

Conclusions and Issues for Further Consideration

In this chapter, we summarize our conclusions and identify issues for further consideration if Congress decides to explore options for relaxing the Mailbox Rule.

Conclusions

Overall, we expect that relaxing the Mailbox Rule will likely have a negative effect on public safety and the security of the mail, as well as increase the number of mail crimes that are not reported, although we speculate that the magnitude of the impact on incidents (based on the limited data available) would likely be moderate. Such an impact would be contingent on the degree of relaxation and whether only major couriers or a range of different types of couriers are allowed to enter the postal market. Whatever the degree of relaxation may be, there is a stronger case for predicting an increase in the cost and complexity of IS investigations.

These findings are based on our analysis of the reported-incidents database and our assessments of key differences between the USPS and private couriers in training, accountability, and oversight. However, it should be highlighted that we had access to minimal data on private courier company practices. We attempted to interview several of the major private courier companies operating in the United States to learn firsthand about the training, guidance, policies, procedures, and technology they currently use to protect the safety and security of their employees, their deliveries, and their customers. However, because we

did not receive a response to our requests, we were limited to publicly available corporate documents about the training and safety and security measures that these companies have undertaken.

If the Mailbox Rule were relaxed, the main risk to the public may be in terms of increased theft at the mailbox. Mail theft plays a role in many broader crimes—including, for instance, identity theft and the fraudulent use of stolen credit cards and pension checks or other payments. An increase in mail theft might occur because a larger number of individuals would be delivering to the mailbox, creating, accordingly, more opportunities for mail theft. In addition, we also expect greater variability in the type of training that personnel have received. This suggests that the training costs and need for training USPS and IS personnel will likely increase. Importantly, these changes raise the question of whether national training standards should be established to help ensure public safety and, if so, who should enforce them.

The other types of mail crime that are most likely to increase following relaxation of the Mailbox Rule are financial crime and the incidence of suspicious items. Our survey results indicate that the public has concerns about the impact on financial crimes, such as identity theft, of relaxing the Mailbox Rule.

These crimes are the most likely to increase because they require the greatest amount of training and detection technology. Hence, proponents of relaxing the Mailbox Rule must address USPS and private courier company training, guidance, policies, and security technology. Ensuring that *all* carriers, USPS and private, have the necessary training, guidance, policies, and technologies in place will require federal regulations. As a result, additional federal, state, and local spending and resources will be needed to enforce such standards. If optimal levels of resources are unavailable, private business—especially smaller couriers with limited financial capacity—will have incentives to cut corners with regard to implementing safety and security training, policies, and technology. Accountability will be a concern, as even publicly traded companies do not receive the same degree of accountability as the USPS does, because of its status as a wholly owned government corporation.

We also examined the IS's arguments against relaxing the Mailbox Rule in terms of its ability to detect and deter crimes and to conduct investigations. We concur that relaxing the Mailbox Rule would likely impair the IS's ability to detect and deter crimes and to conduct investigations by reducing federal jurisdiction over crimes in or at the mailbox or crimes committed using private couriers. Without federal jurisdiction based on mail-crime statutes, the IS has no authority to investigate; it would be limited to providing technical assistance on an ad hoc basis through an interagency task force. Relaxing the Mailbox Rule would also increase the cost and complexity of IS investigations and would deny the IS the ability to track mail crimes nationwide. Although the deterrence value of the Mailbox Rule may be overstated, relaxing it would likely somewhat reduce the IS's ability to deter certain types of crimes that it can currently deter, such as large-scale mail theft and child pornography. Then again, if the Mailbox Rule were relaxed, the IS would have a smaller caseload toward which it could devote a proportionally larger amount of its limited resources.

As just noted, we also conducted a survey of a nationally representative sample of consumers to obtain information on how much support or opposition there may be to opening up access to the mailbox and to better understand the reasons behind their opinions. We found that most consumers oppose the option of opening up access to private couriers—in particular, opening it to parties other than the major carriers in the United States. The majority of respondents opposed opening up access because of security concerns, followed by concerns about increasing the amount of advertising and junk mail they may receive. We found some differences among consumers who lived in urban versus rural locales, but overall there was not strong support for relaxing the Mailbox Rule.

In terms of the experience of the international community, we concluded that comparable lessons learned are limited because of the divergent services provided by non-U.S. postal services and the greater prevalence of mail slots and locked mailboxes abroad. In addition, it is difficult to extrapolate from the experience of other countries because of differences in the characteristics and sizes of their markets. For example, New Zealand Post has a dispersed, less dense population,

and its market is considerably smaller than that of the USPS. That said, a similar set of concerns emerged from our discussions. Similar to the USPS, following 9/11, foreign postal services also implemented training on handling and detecting bio- and other hazardous materials, required their postal investigative services to conduct threat assessments for their facilities, and developed new processes and procedures to address the emerging threat of chemical, biological, and radiological attacks on critical infrastructure. Although they conjectured about the possible impact on public safety and mail security and crime, they noted that, in general, identity theft and theft from the mailbox (e.g., of government checks, credit cards) were a growing concern. In addition, foreign postal services had less visibility into incidents in the market as a whole.

Issues to Be Considered If the Mailbox Rule Were Relaxed

If Congress decides to explore relaxing the Mailbox Rule, a number of issues would need to be addressed. In this section, we offer some observations for further consideration. The discussion that follows reflects the uncertainty about how the Mailbox Rule might be relaxed and the extent and type of diversion to private couriers that might occur. Relaxation could take various forms, such as (1) open access for all, (2) licensed access for private couriers, (3) licensed access for only the largest private courier companies, or (4) restricting access to locked mailboxes. In addition, drawing on the experience of the United Kingdom with postal-service privatization, competition from private couriers may divert some aspects of the mail (e.g., upstream processing and parcels) but not other aspects (e.g., letter volume). The extent to which relaxing the Mailbox Rule will affect incidents, training, and investigations will be contingent on how much diversion occurs and where along the delivery channel private couriers get involved. Therefore, although we have pointed in this monograph to areas of potential increase in the number of incidents, training requirements and costs, and investigation costs and their complexity, it is not possible to quantify these areas without a clear set of options against which to compare them.

That said, we highlight issues to be considered to help mitigate the public safety and security impacts that might occur if the Mailbox Rule were relaxed.

First, Congress may want to consider options for establishing national training standards for private couriers and identify what agency will be responsible for overseeing and enforcing those standards. We believe that there may be a role for the USPS in training private couriers to national standards; however, it might be inappropriate for the USPS to be given the role of *enforcing* those standards against its competitors. Logically, the increase in responsibility needs to have a corresponding increase in funding to account for the new requirements.

Second, because multiple couriers will be involved with processing and delivering the mail, thus raising concerns about decreased reporting of mail crime, a national reporting system may need to be established to allow the IS and DOJ to continue to track mail crime and assess trends over time.

Third, with respect to the issue of federal jurisdiction over the mailbox, Congress may want to consider mandating that the mailbox remain an authorized depository of mail for the purpose of maintaining federal jurisdiction over USPS deliveries to the mailbox and perhaps over crimes against mailboxes themselves (but not over crimes against private courier deliveries to the mailbox, such as theft or tampering).

Fourth, to address the issue that relaxing the Mailbox Rule would result in removing federal jurisdiction over deliveries diverted to private courier companies (except when the crime has an interstate commerce federal jurisdictional hook and an actual interstate commerce nexus), Congress may want to consider increasing the number of mail-crime statutes with a federal jurisdictional hook based on interstate commerce. Congress should decide whether it is indeed inappropriate for the IS to investigate interstate crimes involving the private courier companies that compete with the USPS.

Fifth, to address the public's concerns about security and implications of relaxing the Mailbox Rule, public education and awareness campaigns may need to be implemented to inform consumers about what will change and what that will mean for them (e.g., to whom they

will report mail crime, how to know whether a courier is legitimate). The public awareness campaigns would need to be tailored to address the needs of different populations—for example, for rural populations that may be more resistant to the change.

Finally, if the political will to relax the Mailbox Rule does exist, one option for collecting data in order to quantify the potential impact on public safety and security, as well as other issues, would be to undertake a pilot program in a limited number of areas that would allow individuals to give select parties access to their mailbox. If such a pilot is undertaken, data should be collected on reported incidents (including type of incident), what carrier was involved, characteristics of the incident, to whom the consumer reported the incident, who the responder was, and investigation costs. Doing so is important to quantify the hypothesized impact that relaxing the Mailbox Rule may have on public safety and mail crime. Having such information would, in turn, be crucial in determining the soundness of relaxing the Mailbox Rule and in designing a national implementation.

APPENDIX A

Methods

In this appendix, we summarize the methods we used for each set of analyses.

Methods for Analysis of IS Incident Data

The IS maintains three databases that provide information related to public safety and security: the Fraud Complaint System (FCS), the Financial Crime Database (FCD), and the Suspicious Incident Reporting System (SIRS). Further, within the FCD is a subset of incidents involving volume attacks, and within the SIRS is a subset of explosives incidents involving IEDs/bombs. Taken together, our analysis addresses the following five categories:

- volume attacks, instances in which mail is stolen from a multiple-mailbox location (such as apartment panels)
- fraud data, collected when the IS is contacted about questionable or fraudulent activity involving the mail
- financial crimes, finance-related crimes that have been perpetrated through or aided by the postal system
- suspicious incidents, instances in which there is some problem with a piece of mail and a Postal Inspector visits a site to investigate the contents
- IEDs (bombs), a special subset of the SIRS, involving actual explosives and perceived or explicit explosives threats, which we address as a distinct group.

In addition to using the IS databases, we incorporate information from the U.S. Census Bureau into our analysis to estimate whether each reported incident occurred in a rural or urban ZIP Code,[1] as well as to estimate the projected 2008 median household income within the ZIP Code.[2]

Once each of the data files was received from the IS, we first cleaned the data so that response categories for variables were not duplicated (e.g., the raw SIRS data contained distinct responses on the type of facility to which the inspector responded that included "ISC" and "ISc," both referring to international service centers at airports, and "RESIDENTIAL" and "Residential"). Similarly, the information on first responder and additional agencies involved for each suspicious incident contained multiple variations of the same agency that were combined where appropriate. The IS was entered as "Postal Inspection Service," "Postal Inspection Servcie" [sic], "U S Postal Inspection Service," "U. S. Postal Inspection Service," "U.S. POSTAL INSPECTION SERVICE," "U.S. Postal Inspection Service," "U.S. Postal Inspection Servcie" [sic], "US POSTAL INSPECTION SERVICE," "US Postal Inspection Service," and "USPIS."

The field denoting additional agencies involved was subsequently recoded as a variable with 13 categories by identifying the raw data response as fitting one of the following categories:

1. No other agency included "NULL," "N/A," "None," and the four blank responses.

---

[1] The U.S. Census Bureau defines an urbanized area as consisting of a central city and surrounding areas whose population is greater than 50,000. In addition, other towns outside of an urbanized area whose populations exceed 2,500 are included in the urban population, leaving all other areas rural. According to this definition, the 2000 census indicates that 21 percent of the population lived in rural areas. Because ZIP Codes do not fit standard census measures of geographic space and may overlap both census-defined urban and rural areas, we treat as rural those ZIP Codes in which 50 percent or more of the 2000 population lived in rural areas.

[2] We define *low-income* ZIP Codes as those ZIP Codes with a median household income level at or below the 30th percentile based on projected 2008 income levels from the 2000 census (GeoLytics, 2006). *High-income* ZIP Codes are those with median household incomes at or above the 70th percentile.

2. A.T.F. included ATF.
3. Customs and Border Patrol included CBP.
4. Drug Enforcement Administration included the U.S. Drug Enforcement Administration.
5. F.B.I. included the FBI and the name of a special agent.
6. Federal (other) was a residual category for federal agencies that could not otherwise be categorized.
7. Fire/hazmat included state and local agencies.
8. Health and emergency service included health departments, emergency medical services (EMS), and medical examiners.
9. Joint Terrorism Task Force included JTTF.
10. State/local law enforcement included police, sheriff, constable, and correctional-facility personnel.
11. State/local government was a residual category for otherwise uncategorized or unspecified state or local government agencies.
12. Military included military police, military Criminal Investigation Command (CID), Office of Special Investigations (OSI), any branch of the military services, and bases.
13. USPS included the USPS separately from the IS.

Estimates of the median dollar loss for fraud and financial crimes were based only on those cases in which a dollar amount was reported. In the fraud database, there were a substantial proportion of cases without information (53 percent), while the vast majority of financial crime cases did not include a dollar value (more than 90 percent). Consequently, estimates of loss should be interpreted with significant caution.

The IS-provided data were supplemented with 2000 census–derived data on urban/rural residence and median household income, obtained from the GeoLytics (2006) Planners Package software. Urban/rural residence was based on urban/rural population in 2000, and the median household income was based on the GeoLytics projections for 2008. Data were merged by ZIP Code.

Cleaned and recoded data were then subjected to a range of descriptive analyses and cross-tabulations. Because the data represent

the entire population of incidents collected by the IS, no tests of statistical significance were conducted or required.

Methods for Analysis of Training

We used a combination of methods to examine these issues. We reviewed key USPS training and guidance documents on safety and security training of USPS employees, the mail, and the customer. Taken together, these documents provided critical background information on what training is provided and how it has changed since the 9/11 terrorist attacks. Our review of the training materials also helped in identifying issues to address in the incident-data analyses and interviews.

In addition to reviewing the training documents, we conducted a literature review and Internet search to identify reports that have assessed USPS training and safety measures and that document the USPS's overall role in public safety and security. Using a semistructured interview protocol, we also conducted telephone and in-person interviews with USPS and IS staff to learn about the changes in training that occurred and their overall focus. Assessment of risks to untrained mail carriers (and to USPS personnel) was based on our analyses of the incident data presented in Chapter Two and our assessment of their implications for training.

With respect to considering the safety role and training of the major private couriers, we relied on published summaries of training and safety and security measures that these companies have undertaken. We were unable to interview the major couriers operating in the United States (DHL, FedEx, and UPS) to learn firsthand about the training, guidance, policies, procedures, and technology that they currently use to protect the safety and security of their employees and the mail. Instead, we relied on the limited published summaries available on the Internet regarding the training and safety and security measures that these companies have undertaken.

Methods for Analysis of Investigation Impacts

To assess the impact that relaxing the Mailbox Rule would have on the IS's ability to detect, deter, and investigate mail crimes, we conducted a literature review, examined recent indictments in IS cases, analyzed mail-crime prosecutions according to lead charges listed in the TRAC database, reviewed mail-crime statutes and court decisions, and conducted interviews of USPS and IS leadership.

Following this review, we conducted a legal analysis of the three key points that the IS identified as having an impact if the Mailbox Rule were relaxed. We also examined the possible impact on investigation costs and the reporting and tracking of mail crime.

Methods for Assessing Other Countries' Experiences

The 1997 GAO report surveyed people in eight countries on their beliefs about whether a monopoly can have public safety benefits. We augmented that study (done more than 10 years ago) with a literature review and interviews conducted with personnel from Canada Post and New Zealand Post. We also attempted to conduct interviews with personnel from La Poste, France's mail service, and the Royal Mail of the United Kingdom, but we did not receive a response to multiple queries. Drawing on these sources of information, we examined the role that these services play in public safety, how their approaches to training and safety changed following the 9/11 terrorist attacks and given the heightened security awareness, and their views regarding possible effects on mail crime and public safety in general.

Overview of the American Life Panel Survey Methods

Methods

We initially conducted a literature review, looking for public perceptions of the Mailbox Rule and the USPS generally. We identified two main surveys that examined public perceptions of the Mailbox Rule—

one conducted by GAO (1997) and a survey from Peter D. Hart Research Associates (2003) on behalf of the President's Commission on the United States Postal Service. GAO (1997) completed a survey with 1,013 households in 1996 as part of its report *U.S. Postal Service: Information About Restrictions on Mailbox Access*; this survey focused on the Mailbox Rule. Peter D. Hart Research Associates completed a survey of 760 respondents on May 19 and 20, 2003, with a range of questions about possible improvements of the U.S. Mail system, including two questions about the Mailbox Rule. We also solicited and received some internal USPS market research on the issue, drawn from a survey of 2,021 individuals by Opinion Research Corporation.

In addition, we developed an interview survey using the ALP. The ALP is an ongoing Internet-based panel survey maintained by the RAND Corporation and consists of approximately 1,500 respondents. The panel was originally recruited from respondents age 40 and older in the Monthly Survey of Michigan's Survey Research Center but has subsequently been supplemented with younger respondents so it can be representative of the population aged 16 years and older.[3] Having been selected, these respondents are sent survey questionnaires on a variety of topics several times a month, which they respond to via the Internet to facilitate high response rates in a short period. The majority of the panel members (about 1,250) had Internet access before being selected for the ALP (ALP, 2005). RAND provided free Internet access to the remaining panel members through WebTV and an Internet subscription. This eliminates the bias in sample selection found in many Internet survey panels, which include only computer owners.

Our questionnaire was designed to maintain consistency with the previous surveys then to delve into the reasons behind the decisions. We developed questions similar to those in the GAO survey, the Hart survey, and the USPS internal research to identify changes in opinion. The sample was split into halves for the initial question, with one half getting a question on mailbox access nearly identical to that in the

[3] The Monthly Survey is the leading consumer-sentiment survey that incorporates the long-standing Survey of Consumer Attitudes and produces, among others, the widely used Index of Consumer Expectations.

GAO survey and the other getting a question on mailbox access similar to that used in USPS internal research. This was followed by questions concerning reasons underlying opinions and questions examining perceptions of mail security and demographic information specific to the mail (e.g., type of receptacle). The questionnaire can be found in the next subsection.

Analysis of the data included cross-tabulation and statistical tests for significance. Tests of significant differences also controlled for age, race, gender, family income, and (where appropriate) rural residence. The data were weighted to be nationally representative, using post-stratification weights provided by ALP. Demographic data were also incorporated. ALP provided some of the demographic data directly, including consideration of gender, age, income, race, and location. These location identifiers were linked with data from the U.S. Census Bureau to characterize neighborhoods as rural or urban, as defined in previous chapters.

The final sample that we use for estimation consists of 1,314 respondents interviewed in July 2008 (88-percent response rate). The sample was split, with 49 percent men and 51 percent women.[4] The mean age of the sample was 44.8 years. Family income was calculated categorically, with a median family income between $40,000 and $49,000. The sample was 84 percent white (including Hispanic), with 10 percent black or African American, 2 percent American Indian or Alaskan and 2 percent Asian or Pacific Islander. Finally, the sample was 19 percent rural and 81 percent urban.

Questionnaire

The questions for the entire sample were the same except for question 1. Half of the sample (determined by random) received question 1.1 (the GAO version of this question) and half of the sample received question 1.2 (the USPS version of this question), which provided more detailed information regarding what relaxation of the Mailbox Rule would mean.

[4] Weighted sample characteristics are presented.

1.1) Only the US Postal Service is currently allowed to leave mail in your mailbox. Some people say that it should stay that way. Other people say that some companies should also be allowed to put mail inside mailboxes.

Which of these statements comes closest to your view?

a. U.S. Postal Service only
b. Some parcel companies such as FedEx or DHL should also be allowed
c. Other companies (e.g., local hand delivery firms) should also be allowed
d. Any individual should be allowed
e. Not sure/don't know

SPLIT THE SAMPLE SO HALF GET QUESTION 1.1 AND HALF GET VERSION 1.2:

1.2) As you may know, the Postal Service has the exclusive right to deliver U.S. mail. The Postal Service letter carrier delivers mail into the mailbox, and for some customers through the door slot, and may retrieve mail placed in the mailbox by the customer for collection. No other individual, organization or entity is legally permitted to insert materials into or extract materials from the mailbox.

Some groups are suggesting opening access to mailboxes. Opening access to your mailbox to others, in addition to the U.S. Postal Service, would allow individuals and organizations to insert information directly into your mailbox. The Postal Service would continue to deliver U.S. mail into the same mailbox. Although the federal laws that protect the U.S. Mail would not apply to the items placed in the mailbox by others, state laws may provide protection.

Do you approve or disapprove of having exclusive access to mailboxes?

Would you say you . . .

a. Strongly approve
b. Approve
c. Neither approve nor disapprove
d. Disapprove
e. Strongly disapprove
f. DON'T KNOW

2) Which one of the following would you say would be the strongest reason for supporting a proposal to allow private companies to compete for the opportunity to deliver mail to your home mailbox?

a. Make home *more* secure
b. Make mail *more* secure
c. Would be less expensive
d. Would be faster
e. Prefer private business to the government
f. Not sure/don't know
g. Don't Support

3) Which one of the following would you say would be the strongest reason for opposing a proposal to allow private companies to compete for the opportunity to deliver mail to your home mailbox?

a. Make home *less* secure
b. Could lead to identity theft
c. Make mail *less* secure
d. Would be more expensive
e. Would lead to more "junk mail"
f. Other reason
g. Not sure/don't know
h. Don't oppose

4) Which of these ways best describes how your household gets most of its mail?

a. A mailbox attached to your house
b. A mailbox at the curb
c. A cluster of mailboxes near your home
d. An apartment house mailbox
e. A slot in the door
f. At a U.S. post office
g. Other
h. Not sure/don't know

5) At present, is there a lock on your mailbox, or not?

a. Yes
b. No
c. Do not have a mailbox
d. Not sure/don't know

6) At present, how concerned are you about the security of your mailbox?

a. Very concerned
b. Somewhat concerned
c. Not very concerned
d. Not at all concerned
e. Don't use a mailbox
f. Not sure/don't know

7) At present, how concerned are you about security breaches or crimes committed in the sorting, processing, and transporting of mail?

a. Very concerned
b. Somewhat concerned
c. Not very concerned
d. Not at all concerned
e. Don't use the mail
f. Not sure/don't know

8) How would your level of concern about security breaches or crimes change if other companies were allowed to sort, process, and transport mail?

a. More concerned
b. Would not change
c. Less concerned
d. Don't use the mail
e. Not sure/don't know

9) When your household mails letters or bills, how often are they left in your own mailbox to be picked up?

a. All of the time
b. Most of the time
c. Some of the time
d. Hardly ever
e. Never
f. Not sure/don't know

10) (A matrix question, check one response for each A–D) Would you say your mail service is:

(Strongly Agree) (Agree) (Neither Agree nor disagree) (Disagree) (Strongly disagree) (Don't know)

a. Reliable
b. Secure
c. Private
d. Convenient

APPENDIX B

Detailed Tables of Incidents

Table B.1
Volume Attacks, by Year

Receptacle Type Attacked	Year (%)			
	2004	2005	2006	2007
CBU	10.0	10.2	13.1	12.1
NDCBU	50.7	56.1	61.4	56.9
Post Office Box (5+)	1.7	1.3	1.2	2.9
Apartment panel	25.1	22.2	17.1	19.5
Carrier (robbery)	3.2	1.6	1.8	1.0
Other	9.3	8.6	5.4	7.6
Number of attacks	8,767	9,415	6,375	5,952

Table B.2
Volume Attacks, by Sociodemographic Context

	Sociodemographic Characteristic			
Receptacle Type Attacked	% of All Urban Neighborhood Attacks	% of All Rural Neighborhood Attacks	% of All Low-Income Neighborhood Attacks	% of All High-Income Neighborhood Attacks
Apartment panel	24.0	4.9	11.1	23.7
Carrier (robbery)	2.3	0.0	18.1	0.8
CBU	11.3	11.1	1.5	13.1
NDCBU	52.7	76.6	16.8	56.2
Post Office Box (5+)	1.2	3.9	25.3	0.8
USPS vehicle	4.0	0.0	15.7	2.2
Total	90.0	10.0	1.7	68.3

NOTE: Income columns do not total 100 percent because they account only for low- and high-income neighborhoods.

Table B.3
Types of Financial Crimes

Type of Financial Crime	Description
Account takeover	Access to or manipulation of existing-account information obtained from the mail to commit fraud
Automated teller machine (ATM) or debit card	Theft from mail or nonreceipt of an existing ATM or debit card
Change of address (COA) (USPS, financial institution, or other)	Fraudulent filing of a COA request with the USPS, a financial institution, or other entity
Check fraud (convenience)	Tampering of checks issued by credit-card companies linked to a line of credit (i.e., convenience checks)
Check fraud (counterfeit)	Passing counterfeit checks through the mail
Check fraud (lost or stolen)	Delinquency of receipt or theft of checks sent though the mail
Check fraud (new account)	Opening a checking account using another person's name or address obtained through or using the mail
Check fraud (washed or altered)	Transferring through the mail or obtaining through the mail checks that have been chemically or physically altered to change the intended payee or amount information
Credit card	Credit card not received or stolen through the mail
Electronic payment or transfer	Funds fraudulently transferred from one account to another using information obtained through the mail
Fraudulent application (financial)	Fraudulently obtaining a credit or debit card through falsification of information provided to a credit issuer on an application using the mail to obtain or transfer information or services
Fraudulent application (nonfinancial)	Fraudulently obtaining through the mail stream goods, services, or line of credit by falsifying information provided to a credit issuer on an application
Identity theft	Use of another person's identifying information to fraudulently establish credit, take over a victim's financial accounts, obtain loans, rent apartments, or obtain services with utility companies using or through the postal system
Internet use for fraud	Use of the Internet to open fraudulent bank or credit accounts, purchase merchandise, or obtain other things of value and using the victim's name or address to divert mail matter

Table B.3—Continued

Type of Financial Crime	Description
Mail or telephone order	Use of the mail in any way to aid or perpetrate the use of mail or telephone orders to open fraudulent bank or credit accounts, purchase merchandise, or obtain other things of value and using the victim's name or address
Mail tampering	Mail received open with contents
Mail theft (mail not received)	Incoming or outgoing
Mail theft (mail received open)	Mail received without contents
Money laundering	Use of the mail in any way to aid or perpetrate the disguising of financial assets so that they can be used without legal detection of the illegal activity that produced them
Money order-counterfeit	Use of the mail in any way to pass, tamper with, or obtain counterfeit money orders
Money orders (lost or stolen)	Money orders not received or stolen from the mail
Money orders (fraudulent or illegally purchased)	Use of the mail to illegally purchase or transfer fraudulent money orders
Savings or brokerage	Savings account or brokerage collateral not received in mail
Suspicious activity	Suspicious activity in the environs of customer or USPS mail receptacles

NOTE: Also included in this database but not reported in the table were incidents involving damage to mailboxes, discarded mail, and fire in mailboxes. They were recorded as occurring singly or in combination exclusively with the other two in 0.06 percent (3,369 cases) of all mail-related incidents reported in 2006–2007. These types of incidents were included in conjunction with an additional 2,646 reported financial crimes (0.05 percent of all mail-related financial crimes in 2006–2007), for a total of 0.11 percent of the collected financial crime cases. In 2006–2007, there were 4,653 incidents of damage to mailboxes.

Table B.4
Reported Fraud, by Year

Type of Fraud	Year (%)					Median Reported Loss ($)
	2003	2004	2005	2006	2007	
Advance payment	2.3	2.7	2.3	2.7	3.3	299
Chain letter	0.6	1.2	1.2	1.2	1.5	1
Charity fraud	1.1	1.7	1.5	0.8	0.9	15
Education	0.0	0.1	0.0	0.1	0.0	548
Employment	5.0	4.6	3.6	3.4	3.3	59
False bill or notice	7.4	9.0	6.9	9.0	11.2	80
Harassment	2.8	2.1	1.8	2.0	2.9	30
Investment	0.8	1.0	1.1	1.0	1.0	1,400
Lottery	9.1	10.1	16.3	4.6	6.2	2,828
Medical quackery	0.4	0.5	0.3	0.3	0.4	68
Merchandise or service	58.0	51.0	36.7	50.5	45.6	112
Nigerian fraud	0.2	0.4	2.1	8.5	11.7	2,601
Personals	0.1	0.1	0.0	0.1	0.1	327
Prize or sweepstakes	11.5	13.7	24.4	13.6	9.6	25
Sexually oriented advertising	0.3	0.4	0.3	0.4	0.4	29
Underpaid postage	0.1	0.1	0.0	0.0	0.4	9
Unwanted mail	0.3	0.9	0.9	0.9	1.2	0
Vacation or travel	0.2	0.5	0.4	0.7	0.3	598
Total number of incidents	49,258	44,142	49,352	30,516	32,353	

NOTE: Median loss for all reported fraud between 2003 and 2007 was $116.

Table B.5
Reported Fraud, by Sociodemographic Context

Type of Fraud	Urban (%)	Rural (%)	Low Income (%)	High Income (%)
Advance payment	2.6	2.5	3.7	2.2
Chain letter	1.2	1.0	1.1	1.2
Charity fraud	1.3	1.3	1.3	1.2
Education	0.1	0.0	0.1	0.1
Employment	4.0	4.2	5.4	3.7
False bill or notice	9.0	7.4	10.8	9.4
Harassment	2.5	2.0	2.2	2.5
Investment	1.0	0.9	1.1	1.1
Lottery	9.4	10.8	6.4	9.6
Medical quackery	0.4	0.4	0.4	0.4
Merchandise or service	47.0	44.7	45.7	48.6
Nigerian fraud	5.2	6.1	4.9	5.0
Personals	0.0	0.0	0.1	0.1
Prize or sweepstakes	14.8	17.4	14.9	13.5
Sexually oriented advertising	0.4	0.3	0.5	0.4
Underpaid postage	0.1	0.1	0.2	0.1
Unwanted mail	0.8	0.6	0.8	0.8
Vacation or travel	0.3	0.2	0.2	0.3
Percentage of all reported fraud	84.2	15.8	5.0	95.0

Table B.6
Fraud: How Victim Was Initially Contacted

Type of Contact	Contacted (%)
Email	2.6
Fax	0.1
In person	0.6
Internet	31.2
Magazine	0.8
Newspaper	1.6
Phone	2.1
Private courier	0.0
Radio or TV	0.6
U.S. Mail	54.6
Other	5.7
Number of contacts	222,341

Table B.7
Reported Fraud, by Case and Arrest (%)

Type of Fraud	Percentage of All Fraud Incidents	For Each Fraud Type, What Percentage Becomes a Case or Results in an Arrest
Advance payment	4.1	10.5
Chain letter	0.1	0.8
Charity fraud	0.5	2.9
Education	0.0	6.1
Employment	14.4	23.7
False bill or notice	18.9	14.4
Harassment	0.0	0.2
Investment	0.8	5.2
Lottery	1.6	1.1
Medical quackery	0.9	15.8
Merchandise or service	30.7	4.3
Nigerian fraud	0.0	0.0
Personals	0.0	0.0
Prize or sweepstakes	25.9	11.4
Sexually oriented advertising	0.0	0.8
Underpaid postage	0.0	0.0
Unwanted mail	0.2	1.6
Vacation or travel	1.7	1.7
Total	100.0	

NOTE: Overall, 6.6 percent of all reported fraud incidents become a case or result in an arrest.

Table B.8
Reported Financial Crimes, 2006–2007

Type of Crime	Of Total Crimes Involved (%)	Median Reported Loss ($)
Account takeover	0.19	1,776
ATM or debit card	0.01	997
Check fraud (lost or stolen)	3.57	406
Check fraud (new account)	0.00	1,800
Change of address (USPS)	0.38	1,100
Change of address (financial institution)	0.02	4,391
Change of address (other)	0.21	2,345
Check fraud (convenience)	0.01	3,345
Check fraud (counterfeit)	0.01	703
Check fraud (washed or altered)	0.03	400
Credit card	28.83	83
Damage to mailbox	0.09	516
Discarded mail	0.03	301
Electronic payment or transfer	0.00	2,771
Fire in mailbox	0.00	256
Fraudulent application (financial)	1.13	1,500
Fraudulent application (nonfinancial)	0.58	2,670
Identity theft	1.01	1,561
Internet use for fraud	0.06	850
Mail or telephone order	0.02	263
Mail tampering	1.03	388
Mail theft (mail not received)	96.82	120

Table B.8—Continued

Type of Crime	Of Total Crimes Involved (%)	Median Reported Loss ($)
Mail theft (mail received open)	0.49	90
Money laundering	0.00	699,008
Money order-counterfeit	0.00	5,825
Money orders (fraudulent or illegally purchased)	0.00	124
Money order (lost or stolen)	0.06	179
Savings or brokerage	0.00	28,654
Suspicious activity	0.27	459

NOTE: Number of financial crimes reported = 5,240,605. Median reported loss for all financial crimes = $274,927.

Table B.9
Reported Financial Crimes, by Sociodemographic Context

Type of Crime	Urban (%)	Rural (%)	Low Income (%)	High Income (%)
Account takeover	0.20	0.21	0.12	0.22
ATM or debit card	0.01	0.01	0.03	0.01
Check fraud (lost or stolen)	3.67	3.66	6.50	2.87
Check fraud (new account)	0.00	0.00	0.00	0.00
COA (USPS)	0.41	0.34	0.45	0.40
COA (financial institution)	0.03	0.02	0.03	0.03
COA (other)	0.22	0.19	0.26	0.22
Check fraud (convenience)	0.01	0.01	0.03	0.01
Check fraud (counterfeit)	0.01	0.01	0.02	0.01
Check fraud (washed)	0.03	0.02	0.06	0.03
Credit card	24.85	28.98	31.78	23.50
Damage to mailbox	0.08	0.23	0.05	0.09
Discarded mail	0.03	0.03	0.02	0.03
Electronic payment or transfer	0.00	0.00	0.01	0.00
Fire in mailbox	0.00	0.01	0.00	0.00
Fraudulent application (financial)	0.54	0.47	0.46	0.55
Fraudulent application (nonfinancial)	0.00	0.00	0.01	0.00
Identity theft	1.08	0.97	0.96	1.10

Table B.9—Continued

Type of Crime	Urban (%)	Rural (%)	Low Income (%)	High Income (%)
Internet use for fraud	0.06	0.06	0.06	0.06
Mail or telephone order	0.01	0.01	0.24	0.01
Mail tampering	1.07	1.07	1.50	1.04
Mail theft (not received)	97.34	97.29	97.36	97.30
Mail theft (received open)	0.50	0.55	0.48	0.51
Money laundering	0.00	0.00	0.00	0.00
Money order (counterfeit)	0.00	0.00	0.01	0.00
Money order (fraudulent or illegally purchased)	0.00	0.00	0.00	0.00
Money order (lost or stolen)	0.06	0.07	0.11	0.04
Savings or brokerage	0.00	0.00	0.00	0.00
Suspicious activity	0.26	0.31	0.67	0.24
Percentage of all incidents	89.48	10.52	5.27	62.29

Table B.10
Type of Receptacle Involved in Reported Financial Crimes

Type of Receptacle Involved	Urban (%)	Rural (%)
Apartment panel	20.7	2.9
Business	6.3	3.2
CBU	12.4	7.4
Collection box	4.1	0.7
Curbside	2.7	1.4
Door slot	4.9	0.6
Neighborhood Delivery and Collection Box	1.2	0.5
Post Office Box	0.7	2.1
Parcel locker	0.1	0.1
Porch	15.5	4.7
Residential/Business	6.7	4.7
Rural box	27.2	71.7
Percentage of all incidents	87.9	12.1

Table B.11
Suspicious Incidents, by Year

	Year (%)				
Type of Incident	**2003**	**2004**	**2005**	**2006**	**2007**
Leaking gas	0.4	0.6	1.5	2.4	1.8
Leaking liquid	4.6	4.4	8.9	11.0	16.6
Leaking powder	56.7	64.1	68.6	76.6	71.4
Radiological alert	0.0	0.0	6.0	5.0	5.0
No substance found	0.0	0.0	0.0	0.0	1.4
Threat (no substance found)	18.6	16.5	4.3	2.2	0.5
Threat (substance found)	0.0	0.0	0.0	0.0	0.0
Suspicious substance inside post office facility	10.6	14.3	7.4	1.4	2.5
Suspicious substance outside post office facility	0.3	0.0	3.2	0.8	0.9
Other	8.7	0.0	0.0	0.0	0.0
Number of incidents	1,124	1,466	1,912	2,649	3,016

Table B.12
Suspicious Incidents, by Sociodemographic Context

Type of Incident	Urban (%)	Rural (%)	Low Income (%)	High Income (%)
Leaking gas	1.7	3.5	1.2	2.0
Leaking liquid	11.2	13.3	13.4	12.2
Leaking powder	68.6	71.8	70.1	71.9
Radiological alert	5.4	0.0	0.8	0.1
No substance found	0.6	0.4	0.4	0.5
Threat (no substance found)	5.6	3.2	5.6	6.1
Threat (substance found)	0.0	0.0	0.2	0.1
Suspicious substance inside Post Office facility	4.7	5.7	7.0	4.8
Suspicious substance outside Post Office facility	1.2	1.4	0.4	1.3
Other	0.9	0.8	0.9	1.1
Percentage of all incidents	89.8	10.2	26.7	40.5

Table B.13
Suspicious Incidents: Facility Type, by Year

	Year (%)				
Type of Facility	**2003**	**2004**	**2005**	**2006**	**2007**
Airport Mail Facility (AMF)	4.5	2.8	1.9	2.6	1.5
Annex	4.7	3.1	3.1	3.4	3.1
Bulk Mail Center	1.3	2.8	2.0	1.6	1.8
Company or firm	9.4	7.2	5.0	4.1	3.7
Contract station	0.0	0.0	0.0	0.2	0.2
Educational institution	0.0	0.0	0.0	0.0	0.2
General mail facility	4.7	4.6	4.2	3.1	5.8
Government facility	4.0	5.3	5.8	3.9	4.3
International service center	0.5	1.5	7.6	6.0	5.7
Law enforcement facility	0.0	0.0	0.0	0.0	0.4
P&DC	15.9	17.8	18.7	23.2	21.9
Post Office or station	40.8	38.3	36.1	39.5	39.7
USPS vehicle	0.0	0.0	0.5	0.9	0.9
Residential	8.4	7.2	3.4	5.1	5.4
USPS collection box	0.0	0.0	2.5	1.8	1.7
Other	6.8	9.4	9.0	4.4	3.6
Number of incidents	1,124	1,466	1,912	2,649	3,016

Table B.14
Other Agency Involvement in Suspicious Incidents, by Year

	Year (%)				
Agency	**2003**	**2004**	**2005**	**2006**	**2007**
No others	65.4	60.8	64.8	74.2	80.6
ATF	0.1	0.1	0.0	0.0	0.0
CBP	0.0	0.0	0.6	0.7	0.0
U.S. Drug Enforcement Administration	0.1	0.1	0.0	0.0	0.0
FBI	2.3	2.9	2.4	1.4	0.8
Federal (other)	0.5	1.1	3.5	4.0	4.5
Fire or hazardous materials	8.9	8.5	7.2	5.8	4.0
Health and emergency service	0.7	2.7	1.8	1.0	0.4
JTTF	0.4	0.8	0.6	0.4	0.2
State or local law enforcement	18.2	18.4	15.7	10.7	8.0
State or local government	2.5	3.8	2.6	1.2	1.0
Military	0.6	0.8	0.7	0.4	0.4
USPS	0.1	0.0	0.0	0.1	0.1
Number of incidents	1,124	1,466	1,912	2,649	3,016

Table B.15
Explosives Suspicious Incidents, by Year

	Year (%)				
Type of Explosives Incident	**2003**	**2004**	**2005**	**2006**	**2007**
IED	23.4	20.3	17.8	21.0	14.0
Facsimile or hoax device	2.8	5.7	2.9	2.1	1.7
Mailed explosives	0.0	0.0	0.2	0.2	0.5
Suspicious item or mail	0.0	23.2	70.4	71.1	79.8
Threat	73.8	50.6	7.8	5.7	4.0
Number of incidents	1,032	1,002	935	1,203	1,495

Table B.16
Explosives Suspicious Incidents, by Sociodemographic Context

Type of Explosives Incident	**Urban (%)**	**Rural (%)**	**Low Income (%)**	**High Income (%)**
IED	19.4	19.6	21.0	18.9
Facsimile or hoax device	2.7	2.3	2.4	2.7
Mailed explosives	0.3	0.0	0.3	0.2
Suspicious item or mail	54.7	54.8	52.7	55.9
Threat	22.8	22.9	23.4	21.9
Percentage of all incidents	91.6	8.4	24.6	44.5

APPENDIX C

Guidelines and Training

This appendix describes relevant USPS and other-agency guidance and training.

Table C.1
Summary Table: USPS Guidelines, Training, Policies, and Procedures for Mail Safety and Security

Title	Type	Intended Audience	Description	Source
General employee guidance and training				
Guidance				
Postal Bulletin	Monthly website publication that provides USPS news stories as well as updates on training, guidelines, policies, and procedures	All USPS employees	The USPS uses this to disseminate information on an ongoing basis about safety and security issues, policies, and procedures. Bulletins can include information on such issues as fraud alerts, anthrax response, suspicious-package identification and response, hazardous materials–handling procedures, and other safety and security measures and issues.	USPS (various dates)
Postal Employee's Guide to Safety, Handbook EL-814	Handbook describing general employee-safety procedures	All USPS employees	This handbook provides safety rules and procedures to familiarize USPS employees with the rules that apply to their jobs. It outlines general safety rules, policies, and procedures related to occupational health and safety as well as hazmat spills and leaks.	USPS (2006e)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
City Delivery Carriers Duties and Responsibilities, Handbook M-41	Describes city letter carriers' duties and responsibilities	Urban letter carriers	Outlines the duties and responsibilities of city letter carriers and general precautions they should take to safeguard the mail. It recommends that letter carriers keep all mail for which they are responsible in their possession or locked in a relay box or vehicle at all times and that mail that has not been properly processed by the USPS should never be delivered, and it outlines accountability procedures for such items as keys, postage due, duty, and special-service mail.	USPS (2001)
Supervisor's Safety Handbook, Handbook EL-801	Provides health and safety instructions to USPS supervisors	Supervisors	The purpose of this guide is to emphasize the day-to-day safety and health responsibilities of USPS management. It provides direction on determining accident causes, reporting accidents, inspecting work areas, promoting safety and health, and completing job-safety analyses (JSAs). It provides supervisors with the information and techniques to support current safety and health policies.	USPS (2006b)
Training				
Safety Depends on Me	A video campaign to provide employees with safety and health information	All employees	As part of the USPS's overall employee safety and health communication programs, this video campaign provides employees with safety and health information.	Email communication with USPS (June 30, 2008)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Standard Training Program for City Letter Carriers (Course 44502-00)	Orientation program	Urban letter carriers	This training course is intended to educate new city letter carriers about general work practices as well as how to identify safe work practices. With regard to mail security and safety, it discusses how to identify and handle suspicious and hazardous mail; characteristics of suspicious mail; how to identify hazardous materials; compliance with hazmat guidelines; and applying the principles of aviation security.	USPS (2005a)
Standard Training for Rural Letter Carriers (Course 44503-00)	Orientation program	Rural letter carriers	This course educates new rural letter carriers about how to identify and handle damaged, suspicious, and hazardous mail. Also, it discusses different methods for collecting mail; hazards to be aware of; and procedures to follow when hazardous or suspicious mail is identified in route.	USPS (2006). Facilitator Guide: Standard Training for Rural Letter Carriers.
Manager, Operations Programs Support (Course 11201-52)	A training course for USPS managers that provides instruction on basic management skills as well as instructions for responding to emergencies	Managers	This course provides basic management training and strategic-planning guidance and instruction on managers' roles in national preparedness by providing guidance on responding to emergencies.	USPS (2008). Manager, Operations Programs Support, Facilitator Guide

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Manager, Post Office Operations Development Program (Course 11201-42)	A program for managers of Post Office operations to provide training on basic management skills as well as instruction on responding to emergency situations and promoting the safety and security of USPS employees	Managers	Beyond providing a basic overview of the role of managers in Post Office operations, this course provides instruction on emergency management and monitoring compliance of safety programs, including how to support employee participation in safety programs, managing accident-reduction plans, OSHA inspections, injuries and accidents, environmental programs, and aviation-security programs. It also provides guidance for managers on responding to emergencies.	USPS (2007). Manager, Post Office Operations Development Program, Facilitator Guide
CONCERN: A Management Safety Training Program	A safety training program	Managers	This program discusses policy and provides guidelines and procedures for implementing and conducting CONCERN.	USPS (1982). Management Instruction: CONCERN: A Management Safety Training Program

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Postmaster, Levels 21–22 Development Program (Course 13201-07)	Provides general instruction on postmaster duties and responsibilities, responding to emergency situations, and guidance to promote the safety of USPS employees	Postmasters	Beyond providing general instructions on postmaster roles and responsibilities, management skills, and basic operations and procedures, this course also provides guidance on national preparedness and managing compliance of safety programs. It discusses means of establishing security responsibilities; reviews facility, personal, and vehicle safety measures; and it provides guidance on USPS emergency management and national preparedness. During this course, postmasters also discuss preparing the Integrated Emergency Management Plan (IEMP), implementing EAPs, responding to emergencies, defining the postmaster's role in responding to emergency situations, and aviation security. The training also considers general safety programs to protect the safety of USPS employees.	USPS (2008). Postmaster, Levels 21–22 Development Program, Facilitator Guide
New-Postmaster training	A general training course for new Postmasters	Postmasters	This is a general training course for new Postmasters that includes training on handling suspicious and hazardous mail.	Email communication with USPS (June 30, 2008)
New sales and service associate training	A general training course for new sales and service associates	New sales and service associates	A general training course for new sales and service associates. It includes training on handling suspicious and hazardous mail.	Email communication with USPS (June 30, 2008)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Basic Inspector Training	A basic training course	Postal Inspectors	This is a basic training course that includes components on emergency response.	Email communication with USPS (June 30, 2008)
PPO basic training	A basic training course	Postal Police Officers (PPOs)	This is a basic training course that includes components on emergency response.	Email communication with USPS (June 30, 2008)
Technology for promoting safety and security				
National Training Database (NTD)	A training-tracking tool	Administration	When any training course is completed, its completion and participants must be recorded into the NTD. All training must be documented at the facility level, not the individual level.	Email communication with USPS (June 30, 2008)
High-Efficiency Particulate Air (HEPA) system	Technology used to reduce the risk of USPS employee and customer exposure to biohazards and to prevent cross-contamination of the mail	P&DC	This system removes particulate biohazards and other micron-sized particles from the air, and the USPS uses it for protection from hazardous materials that may be dispersed into the air.	GAO (2002a)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Biohazard Detection System (BDS)	Detects biohazards within USPS processing facilities	P&DC	A special set of equipment that acts as an early-warning system for detecting biohazards within the USPS's processing facilities. It is designed to detect trace amounts of biological agents in the mail stream. The BDS will automatically notify key individuals in the case of an alert. The purpose of the BDS is to reduce the risk to USPS personnel and the general public from the threat of biohazardous materials sent through the mail.	USPS (2006a)
Suspicious mail–specific training				
Guidance Documents				
Decision trees	Decision tree	Managers and supervisors	The documents present separate sets of actions to take, in a flowchart format, during incidents involving a suspicious material. Also, it included different actions for small and large facilities to take during such incidents.	GAO (2005)
Suspicious-mail poster (no longer used)	General suspicious-mail poster	All USPS employees	This poster depicts how to identify a suspicious mail piece and key actions to take on discovery.	GAO (2005)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Suspicious-mail poster: SLAP procedures	Poster about mail with a suspected biological or chemical threat	All USPS employees	Portrays the same information as the 2003 suspicious-mail poster with additional, separate guidance for situations involving a suspected bomb or radiological, biological, or chemical threat.	GAO (2005)
SLAP	SLAP guidance on identifying suspicious mail	Managers and supervisors	Presents characteristics of suspicious mail using the SLAP mnemonic: Shape, Look, Address, features, or Packaging.	GAO (2005)
Suspicious-mail poster: three Ps	Suspicious-mail poster	Managers and supervisors	Presents the three-Ps guidance for responding to suspicious mail and unknown powders or substances	GAO (2005)
Three Ps	Three-Ps guidance on responding to suspicious mail	Managers and supervisors	The three Ps presents "three simple steps" for handling a suspicious package: (1) Package: don't handle it. Isolate the area; (2) People: evacuate the area around the package and notify your supervisor; (3) Plan: contact the IS, police, and community first responders.	GAO (2005)
"Immediate Response Actions: Suspicious Mail and Unknown Powders or Substances"	Poster on immediate-response actions	Managers and supervisors	Presents the three Ps as well as more-detailed instructions for employees, supervisors, and managers on initial actions to take in response to suspicious mail and unknown powders or substances	USPS (2006g), GAO (2005)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Response checklist	Checklist	All USPS employees	Presents actions to take in response to incidents involving suspicious mail or unknown powders or substances.	GAO (2005)
Training				
Suspicious-powder tabletop exercise (no longer used; has been updated)	Tabletop exercise	Managers, supervisors, and support staff	This exercise presents actions to take in incidents involving a suspicious powder leaking from a mail piece. It consisted of scenarios portraying hypothetical incidents and exercises in responding to these different scenarios. It also addressed the decision trees for responding to such events.	GAO (2005)
Suspicious-powder tabletop exercise (has been updated)	Tabletop exercise	Managers, supervisors, and support staff	Updated version of 2003 tabletop exercise. It discusses actions to take during events involving a suspicious powder leaking from a mail piece. It consists of a series of scenarios portraying phases of a hypothetical incident and exercises in responding to these scenarios.	GAO (2005)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Suspicious Mail and Unknown Powders or Substances: Package, Plan, People	A training course that focuses on identifying and responding to suspicious mail and unknown powders or substances	All USPS employees	This training consists of three stand-up talks as well as a DVD containing the suspicious-mail video (USPS, 2006c). Each course addresses (1) the SLAP procedures for identifying suspicious mail and unknown powders or substances, (2) the three Ps for responding to such incidents, or (3) immediate-response actions managers and supervisors should take in responding to such incidents. Each facility is provided with a kit for each supervisor that will include a six-minute IS DVD. The awareness training also includes three short service talks to be given on the three successive first Fridays of the month beginning October 2006. Supervisors and managers are to deliver the service talks and arrange for a viewing of the video by their employees.	USPS (2006c)
Tabletop exercises: Suspicious mail and unknown powders or substances	Active exercises to simulate real-life incidents involving suspicious mail and unknown powders or substances	All supervisors and managers and their employees	Each facility manager is responsible for leading a tabletop exercise and appointing an exercise facilitator who will be responsible for ensuring the completion of all training with the corresponding documentation. These exercises walk employees through the SLAP, three Ps, or immediate-action responses that should be followed in the event that suspicious mail or unknown powders or substances are identified.	USPS (2006c)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Web-based awareness training: suspicious mail and unknown powders or substances	A web-based training program for management to reinforce guidance on identifying and responding to suspicious mail and unknown powders and substances	Supervisors, managers, and executives	This web-based training reinforces the tabletop exercises.	USPS (2006c)
Mandatory stand-up talk (1 of 3): Recognizing Suspicious Mail	Mandatory talks on identifying suspicious mail and unknown powders or substances	All supervisors and managers and their employees	Monthly mandatory talks delivered by managers and supervisors to USPS employees nationally. Focuses on the use of SLAP and the three Ps for identifying and responding to suspicious mail.	USPS (2006c)
Mandatory stand-up talk (2 of 3): Immediate Response to Suspicious Mail and Unknown Powders or Substances	Mandatory talks on responding to suspicious mail and unknown powders or substances	All supervisors and managers and their employees	This mandatory talk provides instruction on what to do once a suspicious letter or package is detected. It indicates the three Ps. It also involves walking employees through three scenarios and how they should respond under each scenario.	USPS (2006c)
Mandatory stand-up talk (3 of 3)	Mandatory talks on whom to contact in the event that suspicious mail and unknown powders or substances are detected	All supervisors and managers and their employees	This mandatory talk reminds employees of basic ways they should respond and whom they should contact in the event that suspicious mail or unknown powders or substances are detected.	USPS (2006c)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Cash security–specific training				
Guidance				
Window Services Crime Prevention Booklet (Publication 348)	Brochure	Sales and service associates and any other USPS employee who accepts mail	This booklet provides instruction for employees who work in Post Offices and accept and handle cash remittances sent through the mail. It instructs employees about precautions to take to prevent crimes from occurring at Post Office service windows.	IS (2007b)
"Registered Mail Security"	Poster on keeping Registered Mail secure	All USPS employees	Presents recommendations on how to keep Registered Mail secure and accountable and procedures for delivering Registered Mail. It also discusses what USPS personnel should never do when handling Registered Mail.	USPS (2005c)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Hazardous materials–specific training				
Guidance				
Hazardous Materials and Spill Response	A handbook providing information on identifying hazardous materials and responding to its release	All USPS employees	Acts as a guide to the proper handling of hazardous materials sent via the U.S. Mail. It is an educational and safety tool. It is intended to train personnel to be able to quickly assess whether an incidental or emergency release is occurring. It describes hazardous materials, how to identify them, what is allowed and prohibited in the mail, what a hazardous release is and how to recognize and define such a release, and actions to take if a leaking package is identified.	USPS (2001)
"Department of Transportation Hazardous Materials Warning Labels and Markings"	Poster describing hazmat labels and markings	All USPS employees	This poster documents the DOT symbols for hazardous materials and explains which substances are prohibited in the mail and which may be permitted in the mail in limited quantities.	USPS (2008b)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Standard Operating Procedures (SOPs) for Handling and Processing Hazardous Materials	Describes the SOPs regarding handling, processing, and transporting hazardous mail	All USPS employees	These SOPs have been developed to assist USPS employees while handling, processing, or transporting mail containing or believed to contain hazardous materials. These procedures provide detailed instructions for the actions that USPS employees must take to minimize potential hazards during processing, distribution, and transportation.	USPS (2006h)
Training				
HAZWOPER First Responder Awareness Level training	A basic course on identifying and responding to hazmat leaks and spills	Mail handlers, supervisors, and other employees who frequently handle packages that may contain hazardous materials	This training course provides guidelines and instruction for responding to mail containing or that may contain hazardous materials. It provides (1) an understanding of hazardous materials, including general categories of hazardous materials accepted into the mail stream; (2) an understanding that hazmat incidents can result in injury and damage equipment and mail if not properly handled; and (3) an ability to identify a potentially hazardous spill or leak. It also outlines facility spill and leak SOPs (e.g., whom to call, necessity of isolating the area, and other elements of the EAP).	USPS (1996)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
HAZWOPER First Responder Operations Level training	A more advanced training course for identifying and responding to hazmat leaks and spills	Maintenance and custodial personnel, supervisors, and other persons designated to manage and clean up incidental spills	This course includes training provided at the awareness level by providing a knowledge of basic hazard- and risk-assessment techniques, selection and use of PPE provided for limited cleanup duties, an understanding of basic hazmat terms, and a thorough familiarization with facility SOPs and EAPs.	USPS (1996)
Emergency response (e.g., anthrax)–specific training				
Guidance				
EAPs	Plans that are required to be implemented in all facilities to promote efficient and effective responses to emergency situations	All USPS employees	EAPs cover a wide assortment of potential emergencies, including fire, explosion, and bomb threats. They address designated actions that management and employees must take to ensure employee safety. A portion of each plan should address actions to take in the event of a hazmat spill and leak in the mail stream or other USPS operation.	USPS (1996)
EAP compliance checklist	A checklist to ensure that facility EAPs address all necessary aspects of emergency response	All USPS employees	This document provides a checklist of contents that a facility EAP should contain.	USPS (1996)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Emergency Preparedness Plan	A plan intended to provide analysis and recommendations as to the technology and process change that should be implemented to reduce risk to employees and customers	All USPS employees	The plan sets in place processes and technological applications that are intended to reduce risks to both employees and USPS customers while maintaining current levels of service. The plan provides, among other information, recommendations as to the combination of technology and processes that should be adopted, how they should be implemented, and how relevant issues should be addressed for future consideration.	USPS (2002a)
Training				
BDS-alert response drills	Training drills to practice interagency (USPS and non-USPS officials) exercises and drills in areas where a BDS has been implemented to prepare for events in which the BDS is alerted	Postal Inspectors, USPS facility employees, local first responders, and public health personnel in areas where a BDS has been implemented	Together, participants perform interagency exercises in every area where a BDS has been implemented. The drills follow established protocols for incidents involving suspected biological threats in USPS facilities. In support of the unified command structure now in place to coordinate multiagency response to significant events, all Postal Inspectors and PPOs are trained in the fundamentals of the National Incident Management System. The drill evaluates the response of the USPS and local officials to a potential positive alert from on-site USPS equipment, which tests for the presence of biohazardous contaminants.	Email communication with USPS (June 30, 2008); IS (2006b)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Manager, Distribution Operations (Module 9: Emergency Management) (Course 51201-35)	A course that instructs managers on how to respond to different emergency situations and develop plans to promote the safety of USPS employees, the mail, and the public during such emergencies	Managers	This course helps participants define their roles in the event of an emergency, explains the purpose of an IEMP, describes a continuity-of-operations plan (COOP), comply with the Postal Alert and Notification System (PANS), and recognize their role in a BDS alert.	USPS. Course 51201-35: Manager, Distribution Operations (Module 9: Emergency Management)
Manager, Distribution Operations (Module 10: Safety and Environment) (Course 51201-35)	A course that instructs managers on how to respond to different emergency situations and develop plans to promote the safety of USPS employees, the mail, and the public during such emergencies	Managers	This course instructs USPS managers on overseeing and monitoring compliance of safety programs; using the Safety Toolkit to review safety documentation; prepare for a Performance Evaluation Guide (PEG) audit or inspection; ensure that the facility is in compliance with OSHA standards; identify opportunities to reduce workplace illnesses and injuries; and effectively participate in various activities promoting safety awareness and accident reduction.	USPS. Course 51201-35: Manager, Distribution Operations (Module 10: Safety and Environment)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Physical security–specific training				
Guidance				
Site-security standards	Handbook outlining physical security requirements	Mandatory for all new facilities and any renovations made to existing facilities	This handbook contains physical security requirements. For example, some of the physical security requirements require perimeter fencing and gates to be 8 feet high and terminate at ground level on a concrete, paved surface or firm, nonshifting soil.	GAO (2004b)
Administrative Support Manual	Manual outlining physical security requirements and duties and responsibilities by position	USPS administrative personnel	This manual outlines physical security requirements to be implemented at facilities, general responsibilities for the various security positions, and practices for providing physical security.	USPS (1999); GAO (2004b)
Policy memoranda	Memos outlining specific security issues and areas of corrective action	Facility managers	USPS officials use these to increase facility managers' awareness of specific security issues and reinforce requirements, such as locking doors, wearing ID badges, and challenging those without IDs. The memoranda reinforce the requirements from the Administrative Support Manual and highlights areas of corrective action based on IS reviews.	GAO (2004b)

Table C.1—Continued

Title	Type	Intended Audience	Description	Source
Training				
Security Control Officer (SCO) training	A course that overviews physical security measures	SCOs	This online training focuses on protecting USPS facilities and personnel, and it includes aspects related to bomb threats and physical security.	Email communication with USPS (June 30, 2008)
Facility training 1 and 2	A course that overviews physical security measures	SCOs	The training focuses on protecting USPS facilities and personnel, and it includes aspects related to bomb threats and physical security. This training updates the previously used SCO training.	Email communication with USPS (June 30, 2008)
Facility-safety course	A course that overviews facility-safety measures	USPS employees	This course includes sections on anthrax awareness, EAPs, and HAZWOPER.	Email communication with USPS (June 30, 2008)
Guidelines				
"It's What's Inside and How It's Packed"	A poster that describes what types of items are allowed through the mail and how to appropriately package such items	General public	This poster provides visual and written descriptions of what is allowed and not allowed to be sent through the mail. It also provides instructions on how to package certain mailable items that may be mistaken as suspicious or hazardous.	USPS (2007)

Table C.2
USPS Guidance and Training for Non-USPS Entities

Title	Type of Guidance	Intended Audience	Description	Source
"Suspicious Mail or Packages"	Suspicious-mail poster	General public	Presents the October 2003 three Ps guidance (see Table C.1) in a poster for USPS employees.	GAO (2005); USPS (2006i)
"Keep the Mail Safe"	Poster providing examples of hazardous materials and detailing which items and how much of each item are permissible via the mail	General public	This poster provides a detailed table of hazardous materials that is and is not permissible through the mail. It provides graphics and examples of different types of hazardous materials. It lists which are permissible through air versus surface mail, documents the maximum amount permitted in the mail, and discusses additional information and documents in which additional information can be found.	USPS (2006d)
"Notice of Reward"	Poster listing each punishable offense under the IS's authority as well as monetary rewards	General public	This poster lists each type of offense for which the IS offers a reward. It provides the name of the offense, a description, and the monetary amount of the reward. This poster is used to spread awareness of the types of offenses and the rewards for information and services leading to the arrest and conviction of any person responsible for an offense.	USPS (2006f)

Table C.2—Continued

Title	Type of Guidance	Intended Audience	Description	Source
"Best Practices for Mail Center Security: Incoming and Outgoing Operations"	A guide for keeping business mail centers safe and secure	Mail-center supervisors	This guide is intended to help mail-center supervisors and their coworkers keep business mail centers safe and secure. The guide provides general advice and recommends protective measures to help assess, prevent, and respond to three types of threats: mail theft, package bomb or bomb threat, and chemical, biological, or radiological threats.	IS (undated)
Don't Let One Phone Call Take It All Away	Poster to raise awareness of resources to help victims of financial mail fraud	Elderly	Provides contact information for elderly consumers who are victims of financial fraud and have lost money due to this fraud.	IS (2001). Don't Let One Phone Call Take It All Away.
"Look Before You Cash!"	Brochure that documents what to look for to guarantee that a Postal Money Order is legitimate	General public	This brochure describes what genuine Postal Money Orders look like and provides guidance on what features to look for before accepting or cashing one. It also provides IS contact information.	USPS (2005c)
"Hang Up on Phone Fraud"	A brochure that describes telemarketing fraud, how to prevent it, and whom to contact for more information	General public	This brochure provides a very brief description of the threat of telemarketing fraud and how consumers can protect themselves against such fraud. It also provides IS contact information in case a consumer wants additional information.	IS (2004b)

Table C.2—Continued

Title	Type of Guidance	Intended Audience	Description	Source
"Safeguard Your Personal Information"	A booklet for consumers about how to protect themselves from identity theft	General public	This booklet provides an overview of identity theft, tips for consumers to protect themselves from it, and what to do when it happens. It also describes how consumers can keep their personal information safe from online prowlers. It provides links to websites that provide additional information about identity theft and contact information for the IS.	IS (2007e)
"Consumer Fraud by Phone or Mail: Know How to Protect Yourself"	A brochure about mail fraud	General public	This brochure provides an overview of the types of consumer fraud that can occur over the phone or via the mail, and it describes the typical pitch that individuals running the fraud scams use. It provides guidance on what to do when scammed, what to do to protect against mail or phone fraud, and whom to contact when it happens.	IS (2006c)
"A Consumer's Guide to Sweepstakes and Lotteries"	A booklet about the risk of sweepstakes or lottery fraud via the mail	General public	A booklet for consumers to use as a guide when responding to sweepstakes offers and for recognizing the difference between legitimate sweepstakes and other types of offers, such as prize promotions, and illegitimate promotions that misrepresent themselves and seek to defraud.	IS (2007d)

Table C.2—Continued

Title	Type of Guidance	Intended Audience	Description	Source
"Ensuring the Security of Apartment Mailboxes"	A brochure that details keeping apartment mailboxes secure	Apartment-building managers and owners	This brochure provides guidance that old apartment mailboxes should be replaced with newer, more-secure unit mailboxes. It also provides guidance on the types of unit mailboxes that are most secure and provides contact information for such mailbox distributors.	USPS (2008). Ensuring the Security of Apartment Mailboxes
"Don't Be the Victim of a Check Scam!"	Brochure describing check scams	General public	This brochure provides a brief overview for consumers by describing what check scams are, how to avoid being a victim of one, the consequences of being involved in one, and whom to contact if it happens.	IS (2008b)
U.S. Postal Inspection Service Guide to Preventing Mail Fraud	A booklet describing mail fraud	General public	This booklet is intended to help consumers and businesses identify different types of mail fraud and describes how to contact the IS.	IS (2007c)

Table C.2—Continued

Title	Type of Guidance	Intended Audience	Description	Source
A Law Enforcement Guide to the U.S. Postal Inspection Service	A guide for federal, state, and local law enforcement agencies; describes IS's role in promoting better collaboration between agencies	Federal, state, and local law enforcement agencies	This guide is designed to help federal, state, and local law enforcement agencies understand how they can assist IS in mail-crime investigations. It also provides information on mail crimes about which a Postal Inspector should be notified. It provides an overview of the IS's authority, its resources to assist local law enforcement, how the IS can help other law enforcement agents, how to detect mail crimes on the street and during searches, how the police can help Postal Inspectors, and different types of mail-fraud schemes. It also describes the IS's crime-prevention materials, jurisdiction, and laws.	IS (2006d)
U.S. Postal Inspection Service Guide to Preventing Mail Fraud (Publication 300-A)	A booklet describing mail fraud	Consumers and Businesses	This booklet is intended to help consumers and businesses identify different types of mail fraud, and it describes how to contact the IS.	IS (2007c). U.S. Postal Inspection Service Guide to Preventing Mail Fraud
Training videos				
Truth or Consequences: Fake Check Scams	Public safety education and outreach video	General public	This video discusses fake-check scams.	USPS email communication

Table C.2—Continued

Title	Type of Guidance	Intended Audience	Description	Source
All the King's Men: Picking Up the Pieces	Public safety education and outreach video	General public	This video discusses fraud schemes that victimize millions of Americans each year, leaving many financially devastated, and urges victims to learn more about their rights.	IS (2006a); USPS email communication
Nowhere to Run: Cross-Border Fraud	Public safety education and outreach video	General public	This video illustrates how U.S. Postal Inspectors created task forces with Canadian law enforcement partners to stop long-distance scams.	IS (2005a); USPS email communication
Web of Deceit: Internet Fraud	Public safety education and outreach video	General public	This video tells the story of a scammer who uses the Internet to victimize unsuspecting consumers around the world until he gets caught in his own web of deceit and provides tips on what to watch out for when doing business on the Internet.	IS (2005b); USPS email communication
Long Shot: Foreign Lottery Scams	Public safety education and outreach video	General public	This video tells the story of a foreign lottery–fraud victim and the con artist behind the scam and provides tips to avoid becoming a victim of this scam.	IS (2004d); USPS email communication
Work-at-Home Scams: They Just Don't Pay	Public safety education and outreach video	General public	This video tells the story of a new type of work-at-home scam and how a young mother gets caught up in it and provides tips on how to avoid being duped by criminals and what to do if it happens.	IS (2004e); USPS email communication

Table C.2—Continued

Title	Type of Guidance	Intended Audience	Description	Source
Identity Crisis: Protect Your Identity	Public safety education and outreach video	General public	This video tells the story of a couple whose credit is ruined and of the criminals who defrauded them and provides tips on how to protect against identity fraud and what to do if it happens.	IS (2004c); USPS email communication
Dialing for Dollars: Telemarketing Fraud	Public safety education and outreach video	General public	This video tells the story of a scam and the lives that are ruined by criminals and provides tips on how to protect against investment fraud and what to do if it happens.	IS (2004a); USPS email communication

Table C.3
USPS Staff Role in Safety and Security

Position Title	Description of Safety and Security Role	Source
USPS staff		
Letter carriers	Beyond general mail-delivery duties and responsibilities, USPS letter carriers are trained to identify and respond to suspicious- and hazardous-mail incidents that may be harmful to the letter carrier and the general public.	USPS (2001a). Handbook M-41; USPS (2005a). Facilitator Guide: Standard Training for City Letter Carriers; USPS (2006). Facilitator Guide: Standard Training for Rural Letter Carriers
Managers	Managers are responsible for managing emergency responses and contacting the IS and emergency responders based on the Postal Inspector's advice.	USPS (2006c)
Supervisors	Supervisors are responsible for ensuring that the employees in their units are trained appropriately to enhance mail safety and security. Supervisors are trained to enhance the day-to-day safety and health of USPS workers, determine accident causes, report accidents, inspect work areas, promote general safety and health, and to complete JSAs. Supervisors are also training in HAZWOPER First Responder Awareness Level training and Operations Level Training.	GAO (2002b)
Area security coordinators	These USPS management officials are responsible for ensuring adequate funding for security; soliciting and encouraging management support in enforcement of security policies and procedures; providing guidance and direction to SCOs; and monitoring and evaluating the effectiveness of security programs.	GAO (2004b)

Table C.3—Continued

Position Title	Description of Safety and Security Role	Source
SCOs	An SCO is usually the installation head or designated manager or supervisor. This official serves as the focal point to help implement security policies and coordinate with the IS as needed on security matters. SCO duties include developing and directing a security program on an ongoing basis; ensuring that appropriate attention is paid to security issues; acting as a liaison to the IS; and conducting an annual facility-security survey and taking corrective action as needed.	GAO (2004b)
Mail handlers	Mail handlers receive training in identifying and responding to suspicious-mail incidents as well as awareness-level training on identifying and responding to hazardous mail.	USPS. HAZWOPER First Responder: Awareness Level Training
Maintenance and custodial personnel	Maintenance and custodial personnel and other persons designated to manage and clean up incidental spills receive both HAZWOPER First Responder Awareness Level training and Operations Level training.	USPS. HAZWOPER First Responder: Operations Level Training
Postmasters	During new-hire orientations, postmasters receive general training that includes training on handling suspicious and hazardous mail.	Email communication with USPS (June 30, 2008).
IS staff		
Postal Inspectors	Postal Inspectors are responsible for initially assessing the threat posed by suspicious mail.	GAO (2005)
PPOs	PPOs provide security at USPS facilities where the IS has determined that risk and vulnerability demonstrate a need for this level of security.	GAO (2002b)
USPS security and safety entities		

Table C.3—Continued

Position Title	Description of Safety and Security Role	Source
Spill and leak teams	Members of the spill and leak teams are trained to respond to hazmat releases and determine whether an emergency exists. These teams can respond to suspicious-mail incidents without spills or leaks. Teams from large facilities can be used in smaller facilities if needed.	GAO (2005)
Mail Security Task Force	This was established in late 2001 to review every plan and approach the USPS has regarding mail security and handling hazardous materials in the mail. The task force was led by the Chief Postal Inspector and included representatives from mail unions, management associations, and the Office of the Inspector General, as well as safety and medical specialists and members of the mailing industry.	USPS (2001b)
Office of National Preparedness	The USPS reorganized its Office of National Preparedness in FY 2007 and placed it under the IS. Responsibilities for the newly restructured office include incident management, infrastructure protection, aviation mail security, preparedness for public health, and emergency-performance measurement. Each of these activities is key in preparing for, responding to, and assisting with recovery from major incidents affecting USPS operations and employees as well as the public.	USPS (2008a)
Global-security and investigation groups	These groups were formed to protect the integrity of Postal Money Orders and other financial instruments targeted by non-U.S. criminals. This initiative resulted in the largest seizure of counterfeit checks and Postal Money Orders in IS history.	USPS (2008a)
Internal-control units	Internal-control units are expected to assess risk and compliance with remittance handling as well as other financial and operational policies and procedures.	GAO (2002a)

Table C.3—Continued

Position Title	Description of Safety and Security Role	Source
IS	The IS provides for the security of the mail and the enforcement of federal mail laws. Since 2003, the IS has worked closely with the USPS to define an expanded role for Postal Inspectors in responding to suspicious-mail incidents, including incidents involving mail leaking an unknown powder as well as nonleaking suspicious mail.	GAO (2005)
USPS facilities		
P&DC	A key mail facility that processes and dispatches some or all incoming and outgoing mail for a designated service area	GAO (2005)
AMF	A mail facility at an airport that receives, concentrates, transfers, dispatches, and distributes principally by air	GAO (2005)
Bulk Mail Center	A highly mechanized mail-processing plant that distributes Standard Mail in bulk form	GAO (2005)
Priority Mail–processing centers	Processes priority mail	GAO (2005)
Post Offices, stations, and branches	Collect, distribute, and deliver mail	GAO (2005)

APPENDIX D

Differences Between FTC and IS Fraud Data

In 2003, the FTC conducted a telephone survey of 2,500 randomly selected adults to estimate the amount of consumer fraud occurring in the United States (Anderson, 2004). Its survey suggested that nearly 25 million adults in the United States were victims of one or more of the consumer frauds that it covered during 2002, with an estimated 35 million incidents of fraud. The 2003 FTC survey of consumer fraud focuses on different types of fraud from those captured in the IS data, with a few exceptions: prizes, false bills, and merchandise or service. These three types of fraud were among the most prevalent in the IS data. A cursory comparison of the estimated number of these types of fraud between the FTC data and the IS data strongly suggests that the IS data significantly underestimate the amount of fraud taking place.

However, one issue that complicates making comparisons between the FTC survey results and the IS incident data is that, in the FTC data, a sample of individuals were asked whether they had been victimized in the previous year, while the IS data contain only cases that (1) were reported to the IS and (2) involved the use of the postal system at some point. This suggests that the IS data will have substantially lower reports of fraud incidence than the FTC data because they are most appropriately viewed as a subset of the FTC data.

The FTC survey also collected information on whether individuals reported the fraud and, if so, to whom they reported it. Based on the FTC results, 8.4 percent of frauds were reported to an "official source" (a local, state, or federal government agency or Better Business Bureau). These types of reports are likely to be similar to the types of

reports made to the IS. The FTC data suggest that we would anticipate roughly 243,600 cases of merchandise or service fraud to be reported to the IS in 2003, assuming that all cases were also linked to the mail. The IS data capture only 11.7 percent, or 28,600, of the anticipated cases. The level of capture for prize fraud is lower, at 3.9 percent, and, for false bills, roughly 1.0 percent.

The IS data also suggest that lower-income victims do not report crimes as frequently as higher-income victims do, based on both the fraud and financial crime databases. The bottom 30 percent of the income distribution contributes only 5 percent of all the fraud and financial crime incident reports, while the upper 30 percent report roughly 60 percent of each. While some of this may be due to differential targeting of schemes based on income, the discrepancy is large enough to strongly suggest otherwise.

Some of the discrepancies are almost certainly due to the types of frauds being captured, even within categories, and whether they meet the requirement of having some link to the postal system. The FTC data suggest that about a third of fraud victims were initially contacted by mail, newspaper, or magazine; the IS data indicate that 57 percent of the fraud incidents had these methods of first contact. Similarly, the FTC data indicate that 16.8 percent of the first contacts were by phone, while the IS incidents include only 2.1 percent of initial contacts by phone.

Comparing the estimated loss per fraud incident by type of incident also suggests differences in the frauds captured. While the FTC-estimated median loss per false bill ($100) approximated the IS loss ($80), the FTC estimate of merchandise or service loss was $40, and the IS estimate was $112. The amount of missing data in the IS reports of loss dollar value (roughly half) suggests that these values should be interpreted with caution and that there may be a reporting bias in the IS data toward higher loss values because information on substantial losses is collected more often than that for minor losses.

Taken together, a comparison of the FTC and IS estimates of specific types of fraud suggests that, as expected, the IS data contain information on a selected subset of these frauds, related both to the requirement of use of the USPS system and the need for fraud to be

reported to the IS. The IS data should not be interpreted as collecting information of consumer fraud more broadly and should be recognized as potentially undercounting the true level of the specific types of mail fraud substantially.

References

"100 Best Companies to Work For," *Fortune*, February 4, 2008. As of September 22, 2008: http://money.cnn.com/magazines/fortune/bestcompanies/2008/full_list/index.html

ALP—*see* "American Life Panel."

"American Life Panel," brochure, Santa Monica, Calif.: RAND Corporation, CP-508(11/05), 2005. As of September 23, 2008: http://www.rand.org/pubs/corporate_pubs/CP508-2005-11/

Anderson, Keith B., *Consumer Fraud in the United States: An FTC Survey*, Washington, D.C., August 2004. As of September 24, 2008: http://purl.access.gpo.gov/GPO/LPS63551

Block, R., "In Terrorism Fight, Government Finds a Surprising Ally: FedEx," *Pittsburgh Post-Gazette*, May 26, 2005. As of September 2, 2008: http://www.post-gazette.com/pg/05146/510879.stm

BLS—*see* Bureau of Labor Statistics.

Bureau of Labor Statistics, "Couriers and Messengers," *Occupational Outlook Handbook, 2008–09 Edition*, last modified December 18, 2007. As of September 2, 2008: http://www.bls.gov/oco/ocos136.htm

Carlstrom, Gregg, "Public Praises Postal Service, Slams FEMA," *Federal Times*, January 28, 2008. As of August 4, 2008: http://www.federaltimes.com/index.php?S=3333067

CDC—*see* Centers for Disease Control and Prevention.

Centers for Disease Control and Prevention, "Q&A About the Cities Readiness Initiative (CRI)," last reviewed July 5, 2007. As of July 31, 2008: http://emergency.cdc.gov/cri/qa.asp

Code of Federal Regulations, Title 39: Postal Service, Part 310: Enforcement of the Private Express Statutes, Section 310.1: Definitions.

———, Title 39: Postal Service, Part 310: Enforcement of the Private Express Statutes, Section 310.3: Exceptions.

Craig, Roger P., and William T. Alvis, "The Postal Monopoly: Two Hundred Years of Covering Commercial as Well as Personal Messages," *University of San Francisco Law Review*, Vol. 12, No. 1, Fall 1977, pp. 57–87.

DHS—*see* U.S. Department of Homeland Security.

DMM—*see* United States Postal Service (2008e).

Federal Trade Commission, *Accounting for Laws That Apply Differently to the United States Postal Service and Its Private Competitors*, December 2007. As of September 19, 2008:
http://www.ftc.gov/os/2008/01/080116postal.pdf

FedEx, "Disaster Relief," web page, undated(a). As of September 19, 2008:
http://about.fedex.designcdt.com/corporate_responsibility/philanthropy/disaster_relief

———, "FedEx Safety and Security Update," web page, undated(b). As of April 29, 2008
http://fedex.com/mq/about/security.html

———, "Our People: Culture of Safety," web page, undated(c). As of September 2, 2008:
http://about.fedex.designcdt.com/corporate_responsibility/our_people/culture_safety

Fields, Gary, "FedEx Takes Direct Approach to Terrorism: Carrier Sets Up Its Own Police Force, Gaining Seat on Regional Task Force Overseen by FBI," *Wall Street Journal*, October 9, 2003.

FTC—*see* Federal Trade Commission.

GAO—*see* U.S. Government Accountability Office.

Geddes, Rick, *Saving the Mail: How to Solve the Problems of the U.S. Postal Service*, Washington, D.C.: AEI Press, 2003a.

———, "Opportunities for Anticompetitive Behavior in Postal Services," Washington, D.C.: American Enterprise Institute, Postal Reform Paper No. 3, May 28, 2003b. As of September 19, 2008:
http://www.aei.org/publications/pubID.17488/pub_detail.asp

GeoLytics, Inc., *2006 Estimates & 2011 Projections and Consumer Expenditures; GeoLytics Planners Package*, East Brunswick, N.J., 2006.

Gottron, Frank, *The U.S. Postal Service Response to the Threat of Bioterrorism Through the Mail*, Washington, D.C.: Congressional Research Service, Library of Congress, CRS report for Congress RL31280, February 11, 2002.

Hart—*see* Peter D. Hart Research Associates.

Hooper, Richard, Deidre Hutton, and Ian R. Smith, *The Challenges and Opportunities Facing UK Postal Services: An Initial Response to Evidence*, London: Department for Business, Enterprise, and Regulatory Reform, May 2008. As of September 19, 2008:
http://www.berr.gov.uk/files/file46075.pdf

IS—*see* United States Postal Inspection Service.

Lacker, Jeffrey M., and John A. Weinberg, "Can the Fed Be a Payment System Innovator?" *Economic Quarterly*, Vol. 84, No. 2, Spring 1998, pp. 1–25.

Lluberes, Andrew L., "Inside the New ATF," *Police Chief*, Vol. 72, No. 11, November 2005, pp. 40–44. As of September 23, 2008:
http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=740&issue_id=112005

Lynch, Lisa M., and Sandra E. Black, *Beyond the Incidence of Training: Evidence from a National Employers Survey*, Cambridge, Mass.: National Bureau of Economic Research, working paper 5231, August 1995. As of September 22, 2008:
http://www.nber.org/papers/w5231

Moore, David W., "High Approval for Most People/Institutions Handling War on Terrorism," Princeton, N.J.: Gallup, November 16, 2001. As of August 4, 2008:
http://www.gallup.com/poll/5062/High-Approval-Most-PeopleInstitutions-Handling-War-Terrorism.aspx

Office of the Governor of the State of California, "Gov. Schwarzenegger Signs Legislation Targeting Large-Scale Identity Theft," press release, September 27, 2006. As of September 23, 2008:
http://gov.ca.gov/press-release/4258

OIG—*see* United States Postal Service Office of the Inspector General.

Peter D. Hart Research Associates, untitled study 7006, OMB 1505-0192, May 2003. As of September 23, 2008:
http://www.treas.gov/offices/domestic-finance/usps/docs/consumer-survey.pdf

Ponemon Institute, "Ponemon Institute Announces 2008 Privacy Trust Rankings of U.S. Government Agencies," press release, Traverse City, Mich., April 7, 2008. As of September 23, 2008:
http://www.ponemon.org/press/Ponemon_2008%20Govt%20PTS%20Study%20FINAL.pdf

Postal Regulatory Commission, "About the Postal Regulatory Commission," undated Web page. As of September 22, 2008:
http://www.prc.gov/prc-pages/about/default.aspx

PRC—*see* Postal Regulatory Commission.

President's Commission on the United States Postal Service, *Embracing the Future: Making the Tough Choices to Preserve Universal Mail Service: Report of the President's Commission on the United States Postal Service*, Washington, D.C., July 31, 2003. As of September 19, 2008:
http://purl.access.gpo.gov/GPO/LPS37032

Public Law 91-375, Postal Reorganization Act, August 12, 1970.

Public Law 93-633 (amended by 95-363), Hazardous Materials Transportation Act, January 3, 1975.

Public Law 109-435, Postal Accountability and Enhancement Act of 2006, December 20, 2006.

Rice, James B. Jr., "Corporate Response to Terrorism, Creating Resilient and Secure Supply Chains," presentation at Global and Homeland Security: Science, Technology, and the Role of the University conference, Massachusetts Institute of Technology, Cambridge, Mass., May 2, 2003. As of September 22, 2008:
http://web.mit.edu/scresponse/repository/mit_050203_rice_scresp.pdf

Russell, Eric, "'Mailbox Bombs' Spur Postal Service to Warn People of Potential Injury," *Bangor Daily News*, June 20, 2008.

Sidak, J. Gregory, "Declaration of J. Gregory Sidak," before the Federal Trade Commission, Washington, D.C., Postal Service Study, Project No. PO71200, c. 2003. As of September 19, 2008:
http://www.ftc.gov/os/comments/USPS%20Study/529332-00015.pdf

Skinner, Brad, Ed Kelly, and William Tenney, "Customs-Trade Partnership Against Terrorism (C-TPAT)," U.S. Customs and Border Protection, briefing for the National Response Framework 2008 Loss Prevention Conference and Expo, Orlando, Fla., June 23–25, 2008.

Soifer, Don, executive director, Consumer Postal Council; John E. Berthoud, president, National Taxpayers Union; Grover Norquist, president, Americans for Tax Reform; James L. Martin, president, 60 Plus; Charles Guy, former director, Office of Economics, Strategic Planning, United States Postal Service; and Rick Geddes, professor, Cornell University, letter to Deborah Platt Majoras, chair, Federal Trade Commission, June 29, 2007.

Stana, Richard M., *Homeland Security: Key Cargo Security Programs Can Be Improved: Testimony Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate*, Washington, D.C.: U.S. Government Accountability Office, GAO-05-466 T, May 26, 2005. As of September 19, 2008:
http://purl.access.gpo.gov/GPO/LPS61823

United Parcel Service of America, "Training and Operations," web page, undated(a). As of April 29, 2008:
http://www.sustainability.ups.com/social/health/training.html

———, "UPS Fact Sheet," web page, undated(b). As of September 22, 2008: http://www.pressroom.ups.com/mediakits/factsheet/0,2305,866,00.html

———, "UPS Relief Efforts," web page, undated(c). As of September 19, 2008: http://www.pressroom.ups.com/landing/0,2111,34,00.html

———, *Operating in Unison: Centennial Edition, 2007 UPS Corporate Sustainability Report*, Atlanta, Ga., August 2008. As of September 2, 2008: http://www.sustainability.ups.com/docs/2007_CSR_PDF_Report.pdf

United States Postal Inspection Service, "Best Practices for Mail Center Security: Incoming and Outgoing Operations," web page, undated. As of September 19, 2008: http://www.usps.com/communications/news/security/bestpractices.htm

———, *Don't Let One Phone Call Take It All Away*, 2001. As of October 6, 2008: http://postalinspectors.uspis.gov/radDocs/pubs/ar02_10.pdf

———, *2002 Annual Report of Investigations of the United States Postal Inspection Service*, December 2002. As of September 23, 2008: http://www.usps.com/postalinspectors/ar02/ar02main.htm

———, *Dialing for Dollars: Telemarketing Fraud*, Chicago, Ill., 2004a.

———, "Hang Up on Phone Fraud," notice, 2004b. As of September 19, 2008: http://www.usps.com/postalinspectors/dial4eng.pdf

———, *Identity Crisis: Protect Your Identity*, 2004c.

———, *Long Shot: Foreign Lottery Scams*, Chicago, Ill., 2004d.

———, *Work-at-Home Scams: They Just Don't Pay*, Chicago, Ill., 2004e.

———, *2003 Annual Report of Investigations*, February 2004f. As of September 23, 2008: http://www.usps.com/postalinspectors/ar03/ar03main.htm

———, *Truth or Consequences: Fake Check Scams*, Chicago, Ill., 2004g.

———, *Nowhere to Run: Cross-Border Fraud*, 2005a.

———, *Web of Deceit: Internet Fraud*, Washington, D.C., 2005b.

———, *All the King's Men: Picking Up the Pieces*, Chicago, Ill., 2006a.

———, *FY 2005 Annual Report of Investigations of the United States Postal Inspection Service*, June 2006b. As of September 24, 2008: http://www.usps.com/postalinspectors/05anrept.pdf

———, "Consumer Fraud by Phone or Mail: Know How to Protect Yourself," publication 281, July 2006c. As of September 19, 2008: http://www.usps.com/cpim/ftp/pubs/pub281.pdf

———, "A Law Enforcement Guide to the U.S. Postal Inspection Service," publication 146, September 2006d. As of September 19, 2008: http://www.usps.com/cpim/ftp/pubs/pub146.pdf

———, *2006 Annual Report of Investigations of the U.S. Postal Inspection Service*, Washington, D.C., January 2007a. As of September 23, 2008: http://www.usps.com/postalinspectors/06FY%20PI%20Annual%20Report.pdf

———, "Window Services Crime Prevention Booklet," publication 348, January 2007b. As of October 6, 2008: http://www.nalcbayarea.com/USPS%20Publications/pub348.pdf

———, "U.S. Postal Inspection Service Guide to Preventing Mail Fraud," publication 300-A, June 2007c. As of September 19, 2008: http://www.usps.com/cpim/ftp/pubs/pub300a.pdf

———, "A Consumer's Guide to Sweepstakes and Lotteries," publication 546, July 2007d. As of September 19, 2008: http://www.usps.com/cpim/ftp/pubs/pub546.pdf

———, "Safeguard Your Personal Information," publication 280, December 2007e. As of September 19, 2008: http://www.usps.com/cpim/ftp/pubs/pub280.pdf

———, *FY 2007 Annual Report of Investigations of the United States Postal Inspection Service*, January 2008a. As of September 24, 2008: http://postalinspectors.uspis.gov/radDocs/pubs/AR2007.pdf

———, "Don't Be the Victim of a Check Scam!" notice 174, July 2008b. As of September 19, 2008: http://www.usps.com/cpim/ftp/notices/not174.pdf

———, *"U.S. Postal Inspection Service Reporting and Regulatory Scope,"* unpublished material provided to the authors, May 19, 2008c.

United States Postal Service, *Postal Bulletin*, monthly publication, various dates. As of September 23, 2008: http://www.usps.com/cpim/ftp/bulletin/pb.htm

———, *The United States Postal Service: An American History 1775–2006*, Washington, D.C., undated(a). As of September 19, 2008: http://www.usps.com/cpim/ftp/pubs/pub100.pdf

———, *Safety Depends on Me*, video, undated(b).

———, USPS marketplace briefing, undated(c).

———, *Management Instruction: Response to Hazardous Materials Releases*, MI EL-810-96-1, February 1, 1996. As of September 24, 2008: http://www.nalc.org/depart/cau/pdf/manuals/Management%20Instructions/MI%20EL-810-96-1.pdf

———, *Administrative Support Manual*, ASM 13, July 1999, updated through October 7, 1999. As of September 24, 2008:
http://www.nalc.org/depart/cau/pdf/manuals/asm/asmtc.pdf

———, *Hazardous Materials and Spill Response*, Washington, D.C., EL-812, March 2001a. As of September 24, 2008:
http://www.nalc.org/depart/cau/pdf/manuals/EL-812%20(2001-Mar).pdf

———, *City Delivery Carriers Duties and Responsibilities*, Washington, D.C., M-41, revised April 5, 2001b. As of September 23, 2008:
http://www.nalc.org/depart/cau/pdf/manuals/m41.pdf

———, "Postmaster General Announces Mail Security Task Force," press release 01-089, Denver, Colo., October 15, 2001c. As of September 24, 2008:
http://www.usps.com/news/2001/press/pr01_089.htm

———, *USPS Is at War Against Terrorism, Working to Keep Employees, the Public, and the Mail Safe*, Washington, D.C., postal bulletin PB 22062, November 1, 2001d.

———, "Emergency Preparedness Plan," press release, March 6, 2002a. As of September 24, 2008:
http://www.usps.com/news/2002/epp/welcome.htm

———, *A Customer's Guide to Mailing*, Washington, D.C., Domestic Mail Manual 100 Series, July 2002b. As of September 19, 2008:
http://www.usps.com/customersguide/_pdf/DMM100.pdf

———, Public Affairs and Communications Office of Strategic Planning, *2003 Comprehensive Statement on Postal Operations*, Washington, D.C., 2003. As of September 22, 2008:
http://www.usps.com/history/cs03/03cs.pdf

———, *Standard Training Program for City Letter Carriers*, Washington, D.C., course 44502-00, January 2005a. As of September 23, 2008:
http://www.nalc.org/depart/citydel/pdf/7610-04-000-7944.pdf

———, "Registered Mail Security," poster 194, March 2005b.

———, "Look Before You Cash!" notice 299, May 2005c. As of September 19, 2008:
http://www.usps.com/missingmoneyorders/_pdf/not299-rev.pdf

———, Public Affairs and Communications Office of Strategic Planning, *2005 Comprehensive Statement on Postal Operations*, Washington, D.C., 2006a. As of September 24, 2008:
http://www.usps.com/strategicplanning/cs05/cs2005.pdf

———, *Supervisor's Safety Handbook*, Washington, D.C., EL-801, April 2006b. As of September 24, 2008:
http://www.nalc.org/depart/cau/pdf/manuals/EL-801%20(2006-Apr).pdf

———, *Suspicious Mail and Unknown Powders or Substances: Package, Plan, People*, Washington, D.C., 2006c.

———, "Keep the Mail Safe," poster 138, January 2006d. As of September 19, 2008:
http://www.usps.com/cpim/ftp/posters/pos138.pdf

———, *Postal Employee's Guide to Safety*, Washington, D.C., EL-814, revised April 27, 2006e. As of September 23, 2008:
http://www.usps.com/cpim/ftp/bulletin/2006/html/pb22179/pb14d-s_002.html

———, "Notice of Reward," poster 296, June 2006f. As of September 19, 2008:
http://www.usps.com/cpim/ftp/posters/pos296.pdf

———, "Immediate Response Actions: Suspicious Mail and Unknown Powders or Substances," poster 205-A, August 2006g.

———, "Standard Operating Procedures for the Handling and Processing of Hazardous Materials," February 6, 2006h. As of October 6, 2008:
http://www.apwu.org/dept/ind-rel/sh/FinalFeb06HAZMATSOP.pdf

———, "Suspicious Mail or Packages," poster 84, September 2006i. As of September 19, 2008:
http://www.usps.com/cpim/ftp/posters/pos84.pdf

———, "It's What's Inside and How It's Packed," poster 37, November 2007. As of September 19, 2008:
http://www.usps.com/cpim/ftp/posters/pos37/welcome.htm

———, "Postal Facts: Facts and Figures About Your Postal Service," web page, c. 2008a. As of September 19, 2008:
http://www.usps.com/communications/newsroom/postalfacts.htm

———, "Department of Transportation Hazardous Materials Warning Labels and Markings," poster 298, April 2008b. As of September 24, 2008:
http://www.usps.com/cpim/ftp/posters/pos298.pdf

———, "Postal Service Exclusive Carrier of Packages to the Last-Mile for DHL," press release 08-062, May 29, 2008c. As of September 22, 2008:
http://www.usps.com/communications/newsroom/2008/pr08_062.htm

———, Comments of the USPS, June 30, 2008d.

———, *Domestic Mail Manual*, Washington, D.C., last amended September 11, 2008e. As of September 19, 2008:
http://pe.usps.gov/text/dmm300/dmm300_landing.htm

United States Postal Service Office of the Inspector General, 2007 employment data from the Talent Management Services, provided to the authors on September 23, 2008.

United States Postal Service staff, meeting with authors, Washington D.C., July 8, 2008.

United States Postal Service v Council of Greenburgh Civic Associations et al., 453 U.S. 114, 101 S. Ct. 2676, June 25, 1981.

UPS—*see* United Parcel Service of America.

U.S. Code, Title 18, Section 1341, Frauds and Swindles.

———, Title 18, Section 1466, Engaging in the Business of Selling or Transferring Obscene Matter.

———, Title 18, Section 1693, Carriage of Mail Generally.

———, Title 18, Section 1694, Carriage of Matter Out of Mail Over Post Routes.

———, Title 18, Section 1695, Carriage of Matter Out of Mail on Vessels.

———, Title 18, Section 1696, Private Express for Letters and Packets.

———, Title 18, Section 1697, Transportation of Persons Acting as Private Express.

———, Title 18, Section 1698, Prompt Delivery of Mail from Vessel.

———, Title 18, Section 1699, Certification of Delivery from Vessel.

———, Title 18, Section 1701, Obstruction of the Mails Generally.

———, Title 18, Section 1702, Obstruction of Correspondence.

———, Title 18, Section 1705, Destruction of Letter Boxes or Mail.

———, Title 18, Section 1708, Theft or Receipt of Stolen Mail Matter Generally.

———, Title 18, Section 1715, Firearms as Nonmailable; Regulations.

———, Title 18, Section 1716, Injurious Articles as Nonmailable.

———, Title 18, Section 1725, Postage Unpaid on Deposited Mail Matter.

———, Title 18, Section 1735, Sexually Oriented Advertisements.

———, Title 18, Section 1958, Use of Interstate Commerce Facilities in the Commission of Murder-for-Hire.

———, Title 18, Section 2251, Sexual Exploitation of Children.

———, Title 18, Section 2252, Certain Activities Relating to Material Involving the Sexual Exploitation of Minors.

———, Title 18, Section 2261, Interstate Domestic Violence.

———, Title 18, Section 2318, Trafficking in Counterfeit Labels for Phonorecords, Copies of Computer Programs or Computer Program Documentation or Packaging, and Copies of Motion Pictures or Other Audio Visual Works, and Trafficking in Counterfeit Computer Program Documentation or Packaging.

———, Title 18, Section 2332, Criminal Penalties.

———, Title 18, Section 2422, Coercion and Enticement.

———, Title 18, Section 2425, Use of Interstate Facilities to Transmit Information About a Minor.

———, Title 18, Section 2511, Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited.

———, Title 18, Section 2512, Manufacture, Distribution, Possession, and Advertising of Wire, Oral, or Electronic Communication Intercepting Devices Prohibited.

———, Title 39, Section 201, United States Postal Service.

———, Title 39, Section 401, General Powers of the Postal Service.

———, Title 39, Section 601, Letters Carried Out of the Mail.

———, Title 39, Section 602, Foreign Letters Out of the Mails.

———, Title 39, Section 603, Searches Authorized.

———, Title 39, Section 604, Seizing and Detaining Letters.

———, Title 39, Section 605, Searching Vessels for Letters.

———, Title 39, Section 606, Disposition of Seized Mail.

———, Title 39, Section 3001, Nonmailable Matter.

———, Title 39, Section 3002, Nonmailable Motor Vehicle Master Keys.

———, Title 39, Section 3002a, Nonmailability of Locksmithing Devices.

———, Title 39, Section 3003, Mail Bearing a Fictitious Name or Address.

———, Title 39, Section 3004, Delivery of Mail to Persons Not Residents of the Place of Address.

———, Title 39, Section 3005, False Representations; Lotteries.

———, Title 39, Section 3007, Detention of Mail for Temporary Periods.

———, Title 39, Section 3008, Prohibition of Pandering Advertisements.

———, Title 39, Section 3009, Mailing of Unordered Merchandise.

———, Title 39, Section 3010, Mailing of Sexually Oriented Advertisements.

U.S. Constitution, Article I, Section 8, Clause 7.

U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, Washington, D.C., 2006. As of September 19, 2008: http://purl.access.gpo.gov/GPO/LPS71533

U.S. Government Accountability Office, *U.S. Postal Service: Information About Restrictions on Mailbox Access: Report to the Chairman, Subcommittee on the Postal Service, Committee on Government Reform and Oversight, House of Representatives*, Washington, D.C.: U.S. General Accounting Office, GAO/GGD-97-85, May 1997. As of September 19, 2008: http://purl.access.gpo.gov/GPO/LPS14677

———, *Diffuse Security Threats: USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis Before Implementation*, Washington, D.C.: U.S. General Accounting Office, GAO-02-838, August 2002a. As of September 19, 2008: http://purl.access.gpo.gov/GPO/LPS30023

———, *U.S. Postal Service: More Consistent Implementation of Policies and Procedures for Cash Security Needed*, Washington, D.C.: U.S. General Accounting Office, GAO-03-267, November 15, 2002b. As of September 27, 2008: http://www.gao.gov/new.items/d03267.pdf

———, *U.S. Postal Service: Better Guidance Is Needed to Ensure an Appropriate Response to Anthrax Contamination: Report to Congressional Requesters*, Washington, D.C., GAO-04-239, September 2004a. As of September 27, 2008: http://www.gao.gov/new.items/d04239.pdf

———, *U.S. Postal Service: Physical Security Measures Have Increased at Some Core Facilities, but Security Problems Continue: Report to Congressional Requesters*, Washington, D.C., GAO-05-48, November 2004b. As of September 19, 2008: http://purl.access.gpo.gov/GPO/LPS55818

———, *U.S. Postal Service: Guidance on Suspicious Mail Needs Further Refinement: Report to the Ranking Minority Member, Committee on Homeland Security and Governmental Affairs, U.S. Senate*, Washington, D.C.: U.S. Government Accountability Office, GAO-05-716, July 2005. As of September 19, 2008: http://purl.access.gpo.gov/GPO/LPS64299

———, *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, Washington, D.C., GAO-08-240, April 2008.

U.S. Statutes, Chapter 43, Statute 2, Section 732, Postal Act, March 3, 1845.

USPS—*see* United States Postal Service.

Weaver, Kimberly, United States Postal Service, email to the authors, August 5, 2008.