

September 5, 2000

PETER A. JACOBSON
SENIOR VICE PRESIDENT,
CHIEF TECHNOLOGY OFFICER

STEPHEN M. KEARNEY
SENIOR VICE PRESIDENT,
CORPORATE AND BUSINESS DEVELOPMENT

RICHARD J. STRASSER, JR.
ACTING CHIEF FINANCIAL OFFICER
AND EXECUTIVE VICE PRESIDENT,

SUBJECT: Audit Report – USPS eBillPay Security and Privacy Issues (Report
Number EC-AR-00-001)

This report presents the results of our audit of the Postal Service's implementation of the USPS eBillPay electronic bill presentment and payment system (Project Number 00SR003EC000). The objective of our audit was to determine whether the Postal Service met information systems security and federal privacy requirements prior to bringing the system online.

We concluded that the Postal Service did not: (1) perform a certification and accreditation of the USPS eBillPay system, (2) identify minimum security requirements in the agreement with CheckFree Corporation, and (3) publish notice of USPS eBillPay in the Federal Register. We made five recommendations addressing these issues. Management generally agreed with our recommendations. Management's comments are included, in their entirety, in Appendix C.

We appreciate the cooperation and courtesies provided by your staff during the audit. If you have any questions or need additional information, please contact Robert Batta, director, Electronic Commerce, or me at (703) 248-2300.

//Signed//

Colleen A. McAntee
Acting Assistant Inspector General
for Audit

Attachment

cc: Richard D. Weirich
James L. Golden
John R. Gunnels

TABLE OF CONTENTS

Part I

Executive Summary	i
--------------------------	---

Part II

Introduction	1
Background	1
Objective, Scope, and Methodology	2
Audit Results	4
Security Issues	4
Recommendations	7
Management's Comments	8
Evaluation of Management's Comments	8
Privacy Issues	9
Recommendation	10
Management's Comments	10
Evaluation of Management's Comments	10
Appendix A. Security Certification and Accreditation Requirements	11
Appendix B. Comparison of Systems of Records	13
Appendix C. Management's Comments	14

EXECUTIVE SUMMARY

Introduction

This report presents the results of our audit of the Postal Service's implementation of USPS eBillPay electronic bill presentment and payment service. The objective of our audit was to determine whether the Postal Service met information systems security and federal privacy requirements when implementing USPS eBillPay.

Results in Brief

While the system sponsor obtained security assurances from CheckFree Corporation prior to implementing USPS eBillPay, we found that the Postal Service did not officially validate, through the existing certification and accreditation process, that the USPS eBillPay system is secure and will adequately protect Postal Service customer data. The Postal Service wanted to quickly bring the system to market and did not follow the existing certification and accreditation process because it would not facilitate expedited system release. The system sponsor also considered USPS eBillPay security a low risk because CheckFree Corporation had provided this type of service since 1997. In addition, the agreement between the Postal Service and CheckFree Corporation provides indemnification in the event CheckFree Corporation's safeguards prove insufficient; however, the agreement did not identify incident reporting and other minimum security requirements for system certification. The security of USPS eBillPay could be strengthened and the interests of the Postal Service could be better protected if the agreement also addressed vulnerability testing. To the Postal Service's credit, the security staff began the certification and accreditation review process shortly after system implementation.

If the Postal Service had validated the assurances it received from CheckFree Corporation concerning the security of the system against its existing security requirements, it may have become aware of the likely threats or ways the system may be misused or how well the mechanisms used to provide protection operate.

We also found that the Postal Service did not publish notice of USPS eBillPay in the Federal Register in accordance with Privacy Act requirements, even though sensitive customer data, such as social security numbers, checking account numbers, and bank routing numbers, are maintained in the

USPS eBillPay "system of records." The Postal Service evaluated an existing "system of records" and believed it covered USPS eBillPay. As a result, interested parties did not have notice of what sensitive data the Postal Service would be collecting, and were not provided the opportunity to submit written data, views, or arguments regarding the use of this information. To the Postal Service's credit, it subsequently drafted a new "system of records," covering USPS eBillPay to consider publishing in the Federal Register.

**Summary of
Recommendations**

We recommend the chief technology officer, in conjunction with the senior vice president, Corporate and Business Development, (a) develop a new process to document system security and meet the intent of system certification and accreditation to be used when partnering with companies operating commercial systems, (b) document any alternative security assurance processes and cross-reference those agreements to the existing certification and accreditation process, and (c) ensure the security assurance process includes participation from the National Information Systems Security office, and the Inspection Service.

We also recommend the acting chief financial officer and executive vice president ensure the Privacy Act officer publish notice of any new system or major changes to an existing system in the Federal Register.

Additionally, we recommend the senior vice president, Corporate and Business Development, hold discussions with CheckFree Corporation regarding additional assurances on how their current business practices meet Postal Service security requirements, to include security incident reporting and vulnerability testing.

**Summary of
Management's
Comments**

Management agreed with four of the five recommendations and their actions met the intent of the fifth recommendation. Management provided clarifying language on their review of CheckFree Corporation's system security. Management's comments, in their entirety, are provided in Appendix C.

**Evaluation of
Management's
Comments**

Management's comments were generally responsive. While management did not fully agree with the finding regarding the Certification and Accreditation of the USPS eBillPay system, actions taken or planned should address the issues raised in this report.

INTRODUCTION

Background

Electronic commerce is one of the most significant threats facing the Postal Service in its more than 200-year history. The Postal Service projects that electronic commerce may cause First-Class Mail revenue to decline by \$33 billion between years 2000 and 2008. To help generate revenue and be competitive in the electronic marketplace, the Postal Service initiated an electronic bill presentment and payment service.¹

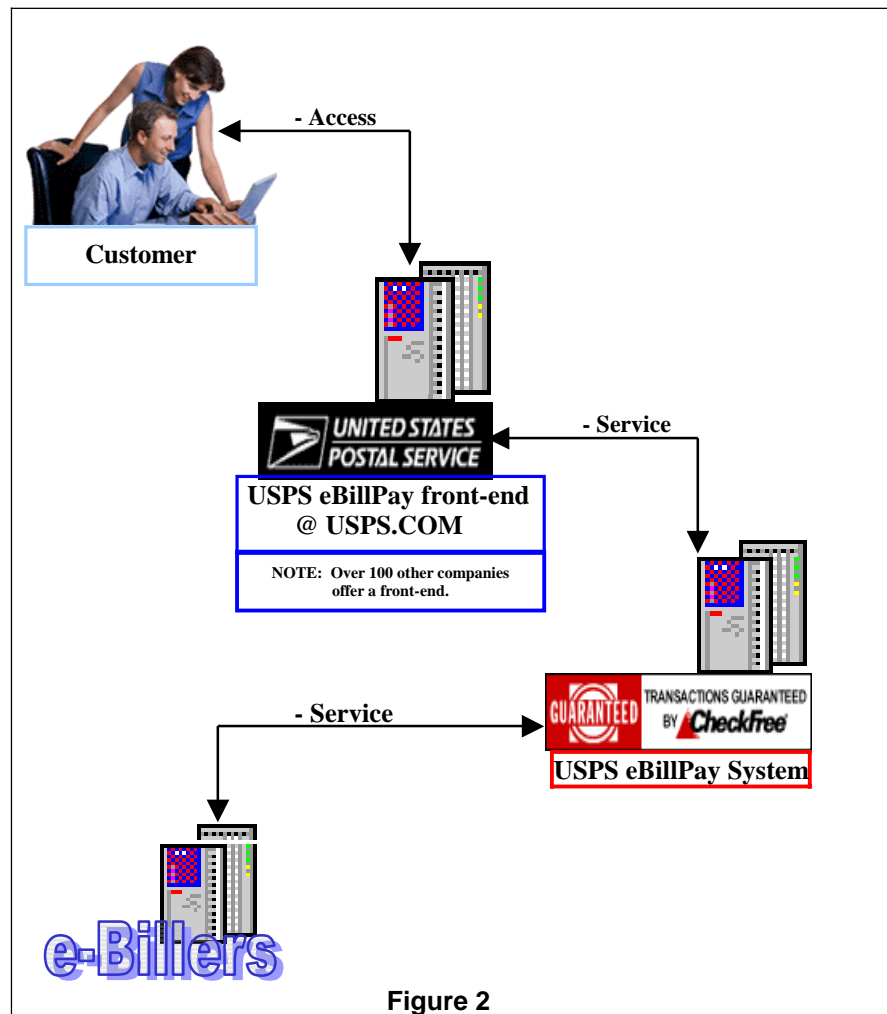
In April 2000 the Postal Service signed an agreement with CheckFree Corporation, and implemented USPS eBillPay. USPS eBillPay allows consumers to pay their bills online through a central, secure Internet web site. Figure 1 describes the bill payment service.



Figure 1

CheckFree Corporation owns and operates the system and infrastructure that support USPS eBillPay (see Figure 2), and offers its electronic billing and payment services through more than 100 other companies. USPS eBillPay maintains sensitive and Privacy Act data owned by the Postal Service and, therefore, is subject to specific Postal Service security and federal privacy requirements.

¹ Electronic bill presentment and payment provides billers a new way to deliver bills and receive payments from customers and provides consumers an easy, secure, and convenient way to receive and pay their bills.



As an Internet service, USPS eBillPay presents security risks that do not exist in paper-based environments. The Internet allows companies to offer electronic commerce services to millions of users, leaving computer systems vulnerable to computer hackers. For example, hackers have stolen thousands of credit card numbers from electronic commerce sites during the last few years. The potential for financial losses from such thefts has raised the issue of financial liability for companies offering Internet services.

Objective, Scope, and Methodology

The objective of our audit was to determine whether the Postal Service met information systems security requirements and federal privacy requirements when implementing USPS eBillPay. During our review, we interviewed Postal Service officials in headquarters and

Raleigh, North Carolina; Inspection Service personnel; and CheckFree Corporation officials. We also reviewed relevant documentation from the Postal Service and CheckFree Corporation, Postal Service security and privacy policies, and the Privacy Act of 1974.

We conducted our audit between April and August 2000 in accordance with generally accepted government auditing standards and included such tests of internal controls as were considered necessary under the circumstances. We discussed our conclusions and observations with appropriate management officials and included their comments, where appropriate.

AUDIT RESULTS

Security Issues

While the system sponsor obtained security assurances from CheckFree Corporation prior to implementing USPS eBillPay, we found that the Postal Service did not officially validate, through the existing certification and accreditation process, that the USPS eBillPay system is secure and will adequately protect Postal Service customer data. In addition, although the agreement between the Postal Service and CheckFree Corporation provides indemnification in the event CheckFree Corporation's safeguards prove insufficient, the agreement did not identify incident reporting and other minimum security requirements for system certification. The agreement also does not address vulnerability tests, which could help strengthen the security of USPS eBillPay and better protect the interests of the Postal Service. To the Postal Service's credit, the security staff began the certification and accreditation review process shortly after system implementation.

Security Certification and Accreditation

Management instruction AS-850-97-3 Security Certification and Accreditation of Sensitive Application and Systems requires the Postal Service to certify and accredit all sensitive computer systems before putting them into production. Certification is an independent analysis of the management, technical, and operational security controls used to determine whether the system meets security requirements. Accreditation occurs after certification and is the official management authorization that appropriate security controls have been implemented to operate the system. The current certification process has 37 management, operational, and technical control security requirements with associated standards that must be met before the Postal Service can accredit a system (see Appendix A). Examples of these requirements include:

- Obtaining security clearances for all personnel working on the system.
- Performing a risk assessment on the system.
- Testing the security of a system.
- Establishing a security plan that addresses security requirements.

While the Postal Service obtained security assurances from CheckFree Corporation, we found that the Postal Service did not certify and accredit USPS eBillPay in accordance with existing Postal Service requirements before bringing it online. The security assurances included CheckFree Corporation's Statement of Accounting Standards No. 70² and an indemnification clause in the agreement in the event CheckFree Corporation's safeguards proved insufficient.

If the Postal Service had validated the assurances it received from CheckFree Corporation concerning the security of the system against its existing security requirements, it may have become aware of the likely threats or ways the system may be misused or how well the mechanisms used to provide protection operate.

The Postal Service did not follow the existing certification and accreditation process because it wanted to bring the system to market quickly. In addition, the system sponsor considered USPS eBillPay security a low risk because CheckFree Corporation had provided this type of service since 1997. Thus, the system sponsor made a business decision to focus on the operational, logistical, and legal aspects of USPS eBillPay and agreed to perform the certification after system implementation.

We recognize that CheckFree Corporation's system may have been in operation for some time and have security measures in place that may meet some Postal Service requirements. However, the Postal Service should have considered all aspects of its security and privacy requirements for protecting customer data in addition to the assurances provided by CheckFree Corporation and included the National Information Systems Security office earlier in the process.

We also recognize that the management instruction applies to systems developed for and by the Postal Service, and that it does not specifically address existing systems operated by private corporations which partner with the Postal Service. However, it is the only guidance the Postal Service has in place to ensure the security functions of a

² In 1993, the Auditing Standard Board of the American Institute of Certified Public Accountants issued Statement of Accounting Standards No. 70 (SAS 70), "Reports on the Processing of Transactions by Service Organizations," which provides guidance to companies that outsource accounting tasks to service organizations.

system are sufficient to protect the system and its information, and that implementation decisions are made in full consideration of Postal Service security requirements and standards.

Post Implementation
Actions

After official notification of USPS eBillPay implementation, the National Information Systems Security office and the Inspection Service began assessing security as part of the certification and accreditation process. They found:

- While Postal Service certification requirements indicate that no one should work on a system until they receive the proper security clearance, at least 600 CheckFree Corporation employees without the required security clearances have access to Postal Service customer data.³
- Despite the Postal Service's certification requirement that all security incidents be reported, there are no procedures in place for CheckFree Corporation to notify the Postal Service of security incidents.
- [REDACTED] [REDACTED] [REDACTED] [REDACTED]⁴
[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED].

Security Requirements
in the Agreement with
CheckFree Corporation



In reviewing the agreement between the Postal Service and CheckFree Corporation, we determined security requirements, as detailed in the agreement, were not sufficient to protect the Postal Service's interests and customer data. The agreement provides indemnification to the Postal Service in the event CheckFree Corporation's safeguards prove insufficient; however, the agreement did not identify incident reporting and other minimum security requirements for system certification. The agreement also does not address vulnerability tests which could help strengthen the security of USPS eBillPay and better protect the interests of the Postal Service. Therefore, the Postal Service may not be able to require CheckFree Corporation

³ All CheckFree Corporation employees undergo background checks, credit checks, and drug testing. The Inspection Service is currently in the process of working with CheckFree Corporation to determine which of its employees have access to USPS eBillPay and, therefore, will require a security clearance. In addition, the Inspection Service is determining whether CheckFree Corporation's clearance procedures are adequate to meet the intent of the Postal Service's security requirements.

⁴ A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.

to meet minimum requirements for security of data, system access, telecommunications, networks, software, and personnel.

[REDACTED], [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED].

In addition to the alliance agreement, the Postal Service provided us its draft security exhibit for review and comment after it implemented USPS eBillPay. In our May 2000 response, we concluded that while security issues were generally addressed, clearer and specific criteria and requirements should be added to the exhibit. Specifically, the exhibit did not address or reference Postal Service internal security policies, standards, and procedures that CheckFree Corporation should follow. We also observed the exhibit only addressed physical security and suggested the Postal Service incorporate minimum security requirements in the exhibit. These would include security of data, system access, telecommunications, networks, and software security as well as training, personnel security, and other specific security requirements.

Recommendations

We offer the following recommendations.

We recommend that the senior vice president, chief technology officer, in conjunction with the senior vice president, Corporate and Business Development,

1. Develop a new process to document system security and meet the intent of system certification and accreditation to be used when partnering with companies operating commercial systems.
2. Until a new process is developed, document any alternative security assurance processes and cross-reference those agreements to the existing certification and accreditation process.
3. Ensure the security assurance process includes participation from the National Information Systems Security office, and the Inspection Service.

We further recommend the senior vice president, Corporate and Business Development,

4. Hold discussions with CheckFree Corporation regarding additional assurances on how their current business practices meet Postal Service security requirements, to include security incident reporting and vulnerability testing.

**Management's
Comments**

Management agreed with the recommendations and stated they were already using eBillPay to help develop an alternative process.

Management also stated that while they did not use the certification and accreditation process to officially validate CheckFree's system, they did perform an initial assessment of CheckFree's system which revealed that CheckFree adhered to high security standards sufficient to protect Postal Service data.

Management's comments, in their entirety, are included in Appendix C.

**Evaluation of
Management's
Comments**

Management asserts that their initial assessment of CheckFree's system revealed that CheckFree adhered to high security standards sufficient to protect Postal Service data. However, management could not provide sufficient documentation to support this assessment, nor documentation to support the business decision to bypass the existing certification and accreditation process. Additionally, management's rationale for bypassing the existing certification and accreditation process only came to light during draft report discussions, and, therefore, the new information provided in support of their verbal assessment was not validated during this review. However, we considered management's actions, taken and planned, responsive to the issues raised in this finding.

Privacy Issues

We also found that the Postal Service did not publish notice of USPS eBillPay in the Federal Register in accordance with Privacy Act requirements. This occurred because the Postal Service believed an existing, published "system of records," (Marketing Records) met the Privacy Act requirements. To the Postal Service's credit, it drafted a new "system of records," (Customer Records) specifically covering USPS eBillPay to consider publishing in the Federal Register.

The Privacy Act of 1974 requires agencies to publish notice in the Federal Register of any new "system of records" or changes in an existing "system of records" at least 30 days before the system becomes operational. It also requires that interested persons have an opportunity to submit written data, views, or arguments to the agency. In addition, pursuant to this act, the Postal Service's Administrative Support Manual requires when an agency (a) expands the types or categories of information maintained in a "system of records" or (b) alters the purpose for which the information is used, it must publish the "system of records" in the Federal Register before implementation. .

In comparing Marketing Records with Customer Records, Customer Records expanded the categories of information and changed the purpose of the system. Only two categories (customer name and address) were similar between the two "systems of records," and Customer Records added nine additional categories of information including social security numbers, checking account numbers, bank routing numbers, etc. The purpose of Customer Records was to provide electronic billing and payment services to Postal Service customers, which was not covered in Marketing Records. A list of categories of information and a description of the purpose of each "system of records" is included in Appendix B.

Because the Postal Service did not provide notice in the Federal Register, interested parties did not have an opportunity to learn what information the Postal Service would be collecting, and to submit written data, views, or arguments regarding the use of this information. As the Postal Service competes in the electronic marketplace, it is even more exposed to public scrutiny and possible criticism

by competitors and other organizations. This potentially puts the Postal Service's reputation of public trust at risk.

Recommendation

We recommend the acting chief financial officer and executive vice president,

5. Ensure the Privacy Act officer publish notice of any new system or major changes to an existing system in the Federal Register.

**Management's
Comments**

Management agreed with the intent of this recommendation and stated they continue to believe that it was appropriate and legally sufficient to rely on the existing system of records for Marketing Records as the basis for Privacy Act compliance for USPS eBillPay. Management further stated that a new system of records was drafted specifically for USPS eBillPay to meet perceived public concern about the routine uses prescribed for the Marketing Records system of records.

**Evaluation of
Management's
Comments**

Management's actions meet the intent of the recommendation.

APPENDIX A

[REDACTED]

[REDACTED]		
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	

APPENDIX B. COMPARISON OF SYSTEMS OF RECORDS

Marketing Records (Existing)	Customer Records (Draft)
Categories of Information NOTE: The bolded items represent those categories that are similar	
<ul style="list-style-type: none"> • Customer name and address • Customer profile and telephone number • Description of items ordered and prices • Payment type • Credit card payment information • Order fulfillment information • Inquiries on status of orders 	<ul style="list-style-type: none"> • Customer name and address • Home and work phone number • Date of birth • Driver's license number • Social security number • E-mail address • Service billing information (checking account number and bank routing number) • Service user name/ID and password • Consumer's bills registered with the service • Bill detail • Bill summaries
Purpose	
Operate a subscription service of services for customers who remit money for a particular product or products.	Provide electronic billing and payment services to postal customers.
Maintain a file to send product announcements and sales literature to customers or subscribers.	
Serve as a source for statistical data for research and market analysis, billing and inventory data, and mailing basis for product shipment.	
Identify discrete groups of customers/subscribers for better order control and service.	

APPENDIX C. MANAGEMENT'S COMMENTS



September 5, 2000

COLLEEN A. MCANTEE

SUBJECT: Management Comments on Transmittal of Draft Audit Report – USPS eBillPay Security and Privacy Issues (Report Number EC-AR-00-DRAFT)

Below are your recommendations on the USPS eBillPay security and privacy audit followed by management's responses:

Recommendation No. 1

Develop a new process to document system security and meet the intent of system certification and accreditation to be used when partnering with companies operating commercial systems.

Recommendation No. 2

Until a new process is developed, document any alternative security assurance processes and cross-reference those agreements to the existing certification and accreditation process.

Recommendation No. 3

Ensure the security assurance process includes participation from the National Information Systems Security office and the Inspection Service.

Recommendation No. 4

Hold discussions with CheckFree Corporation regarding additional assurances on how their current business practices meet Postal Service security requirements, to include security incident reporting and vulnerability testing.

Management's Response:

Management agrees with the first four recommendations, and we would like to add the following comments:

With regard to Recommendation No. 2, management is already using eBillPay to help develop an alternative process. With regard to Recommendation No. 3, we agree insofar as it applies when partnering with companies operating commercial systems.

Although we did not use the Certification and Accreditation process to officially validate CheckFree's system, the Postal Service did perform an initial assessment of CheckFree's system. This assessment revealed that CheckFree adhered to high security standards sufficient to protect USPS data. These standards include annual audits by Deloitte & Touche for CheckFree's compliance with Statement of Accounting Standard Number 70 (SAS 70), which includes security controls and policies. Additionally, the Office of the Comptroller of the Currency periodically audits CheckFree on behalf of the Federal Reserve and the Federal Deposit Insurance Corporation covering data security, business resumption planning, and financial regulatory compliance.

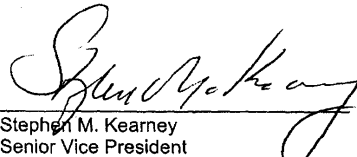
CheckFree is the industry leader for financial electronic commerce services and products, and has been an electronic payments processor since 1981. CheckFree services 3.5 million consumers, and has contracts with 157 of the nation's top billers and nearly 200 consumer service providers, including USPS eBillPay, banks, brokerage firms, and Internet portals.

Recommendation No. 5

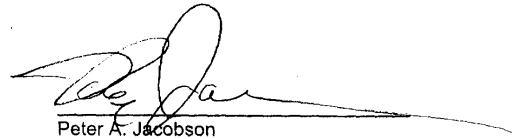
Privacy Act officer publish in the Federal Register notice of any new system or any major change to an existing system containing Privacy Act data.

Management's Response:

The Postal Service continues to believe that it was appropriate and legally sufficient to rely on the existing system of records for Marketing Records as the basis for Privacy Act compliance for USPS eBillPay. The Postal Service undertook to draft a new system of records specifically for USPS eBillPay to meet perceived public concern about the routine uses prescribed for the Marketing Records system of records.



Stephen M. Kearney
Senior Vice President
Corporate and Business Development



Peter A. Jacobson
Senior Vice President
Chief Technology Officer

**Major Contributors to
This Report**

[REDACTED]
[REDACTED]
[REDACTED]