

Office of Inspector General

Protection of Credit Card Numbers

05-01



April 21, 2005



June 2, 2005

The Honorable Nancy C. Pellet
Chairman of the Board and
Chief Executive Officer
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102

Dear Ms. Pellett:

The Office of the Inspector General has completed an inspection of Agency credit card security controls. The objective of this inspection was to evaluate the controls over sensitive credit card information generated by Bank of America for the Farm Credit Administration.

We interviewed FCA staff responsible for travel and purchase cards and account reconciliations. We reviewed internal procedures for credit card programs and previous work performed by the OIG. The inspection followed the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency *Quality Standards for Inspections*.

We found that Bank of America was unresponsive to previous account maintenance requests by the Agency's Official Point of Contact. Actions taken by FCA will improve present data security conditions.

I would be pleased to meet with you and discuss the report at your convenience.

Respectfully,

Stephen G. Smith
Inspector General

Enclosure

BACKGROUND

The Farm Credit Administration (FCA or Agency) is an independent Federal bank regulatory agency that employs approximately 280 employees. Almost all employees have government travel credit cards. Additionally, 39 employees have credit cards for agency purchases.

FCA uses the services of Bank of America (BOA) for travel cards, purchase cards, fleet cards, and convenience checks. FCA's arrangement for these credit card services is under a tag along interagency agreement with the Department of Interior's (DOI) contract with BOA through the U.S. General Services Administration (GSA). FCA's original arrangement with DOI/BOA was for 6 years. In November 2004, FCA continued BOA services for another year, again under DOI's contract. This arrangement ends in November 2005.

The Office of Chief Financial Officer (OCFO) is responsible for travel card management for the agency, including issuing travel cards, closing those accounts, and reviewing travel account activity. Further, OCFO performs the reconciliations of billing statements from the Bank of America for purchase card accounts with FCA's financial management system. Within OCFO, the Financial Operations Specialist is responsible for all travel card duties and responsibilities and the Designated Billing Officer (DBO) is responsible for reconciling the agency's purchase card accounts.

The Office of Chief Administrative Officer (OCAO) is responsible for purchase card management for the agency, including: issuing purchase cards, fleet cards and convenience checks, closing purchase accounts, and reviewing purchase account activity. The Agency's Official Point of Contact (AOPC) is responsible for the maintenance of all purchase and fleet credit card accounts.

BOA provides an online system called EAGLS for account management. Designated officials from agencies can obtain up-to-date account information, manage administrative issues concerning accounts and run reports on account holders, merchants, or offices for internal controls or analysis.

SCOPE AND OBJECTIVE

The objective of this inspection was to evaluate the controls over sensitive credit card information generated by Bank of America for FCA. The inspection was limited to communications between FCA and Bank of America, we also spoke with staff from the Farm Credit System Insurance Corporation (FCSIC) since FCSIC had erroneously received FCA credit card information. Specifically, we evaluated the controls for safeguarding agency and employee credit card information.

Fieldwork began in December 2004 after an entrance conference was held on December 2nd. We performed the following: interviewed FCA staff responsible for travel cards, purchase cards and account reconciliations; reviewed internal procedures for credit card programs; reviewed previous work performed by the OIG; interviewed BOA staff; reviewed BOA documentation sent to FCA and the documentation available on-line through EAGLS. The inspection was completed in accordance with the PCIE/ECIE Quality Standards for Inspections.

FINDINGS AND RECOMMENDATIONS

BOA Is Unresponsive to Agency Service Requests

BOA's poor customer service has hindered FCA's ability to properly manage credit card accounts. Our review found that the difficulty in getting BOA to fulfill customer service requests has led to improper mailings of sensitive information and incorrect account information.

BOA Sent Sensitive Credit Card Information to Unauthorized Parties

On multiple occasions, the Farm Credit System Insurance Corporation (FCSIC) received mail from BOA that included raw data reports containing detailed credit card information for FCA employees. On one occasion, FCSIC received similar detailed raw data for the Commodity Futures Trading Commission (CFTC). BOA sent these reports to the attention of FCA's former AOPC who left the agency in August 2000.

The raw data reports encompass all agency credit card accounts (both open and closed). The reports included name, address (home address and social security numbers for travel cards), account number, and credit limit. According to BOA, a BOA contractor generates and mails the reports through a computerized system. Because there is no manual oversight, BOA cannot detect mailing errors. BOA indicated that FCSIC was in BOA's records as being under FCA's hierarchy. BOA also had the former FCA employee (who separated from FCA in 2000) as the point of contact for both FCA and FCSIC. BOA explained that since both entities had the same point of contact and the same address, both agencies' reports were put in the same envelope. While this explanation appears reasonable, we found the raw data reports are not consistently mailed together. It also does not explain why FCSIC received the CFTC report.

The raw data reports are difficult to read and extract useful information. This same information in a more useful format can be self-generated through the online system or obtained from the billing statements received by FCA. After discussing our observation with FCA managers and responsible staff, FCA directed BOA to stop sending the raw data reports.

Poor Customer Service Makes Account Management Difficult

FCA must continually work with BOA personnel to maintain the accuracy of agency account information. FCA's AOPC and FCSIC personnel stated that obtaining assistance from BOA is time consuming and follow up is required because there is a lack of confidence that changes will be made by BOA. We were informed of repeated instances where BOA was not responsive to agency requests for assistance. FCA and FCSIC staff gave the following examples:

- As noted earlier, BOA had FCA's and FCSIC's official agency point of contact as an employee who left FCA almost 5 years ago, although personnel from both agencies stated that they had repeatedly requested that BOA change the point of contact. BOA finally changed the point of contact on February 10, 2005 after the OIG and the AOPC contacted BOA directly. However, BOA put the former point of contact as the backup for FCA, although BOA was informed that he was no longer with the Agency.
- FCSIC severed all financial services with FCA in January 2002, and all services with BOA in September 2004. However, according to current BOA records, FCSIC is still under FCA's hierarchy.

- The AOPC informed the OIG that he experiences poor customer service from BOA in responding to requests for changes, updates or assistance with EAGLS applications and account maintenance. He noted requests to BOA are frequently time consuming and cumbersome. Specific examples included:
 - BOA's ordering process for convenience checks is flawed and requires personal follow-up by FCA because the ordering forms are inaccurate. FCA has spent a large amount of staff resources over an extended period attempting to remedy the problem with BOA.
 - BOA provided inaccurate directions for resolving problems encountered with EAGLS and requests for changes.
 - The EAGLS system does not always retain changes made by FCA employees online. A recent incident showed that although FCA "submitted" a hierarchy change, the information reverted back to the original data.

Similarly, the OIG documented several instances where BOA was not responsive:

- Accounts that were closed by FCA personnel through EAGLS as long as six years ago, still appear in the EAGLS database and have not been purged. The BOA representative assigned to FCA stated that closed accounts are purged after being closed for 3 years.
- BOA did not have a backup representative at the beginning of the fieldwork. The BOA representative for FCA was out of the office for an extended period of time and some areas of fieldwork were delayed until she returned. At the end of the fieldwork, the BOA representative offered another BOA employee to assist the OIG, but when an attempt was made to contact that employee, he was out of the office for an extended period.

BOA's unresponsiveness results in inefficiencies, inaccuracies, and contributed to the improper mailing of sensitive account information.

Agreed Upon Action

1. *FCA will review available options for credit card services and, to the greatest extent possible, require performance metrics in any new agreement with a credit card provider.*

FCA Can Take Actions to Mitigate Risks of Sensitive Information Being Exposed

Account Information Should Be Kept Current

FCA should ensure that account information for all credit cards are kept up-to-date and that closed accounts that contain personal information are purged as soon as practical. The EAGLS system contains outdated, erroneous, or missing information about cardholders' offices or divisions. With the recent changes to EAGLS, FCA can correct much of this information online. The AOPC stated that he has nearly completed the updating of the hierarchy designations for purchase accounts since he is now able to do this online.

We found a large number of closed accounts in the EAGLS online database, some that were closed as long as 6 years ago. There were 210 closed FCA travel accounts and 26 closed purchase accounts in the EAGLS system. The closed travel accounts have former employees' personal addresses and social security numbers. We also found six FCSIC employees are

listed under the FCA hierarchy with open travel card accounts. These accounts should not be under FCA, and should have been closed since FCSIC stopped using BOA services this past fall. During the inspection fieldwork, the Financial Operations Specialist closed these accounts. Allowing an individual's personal information to be maintained in an online database when the accounts are no longer needed creates an unnecessary risk to former cardholders' personal information. All closed accounts should have the cardholder's personal information immediately removed from the EAGLS online system and the account purged after a reasonable period of time.

Agreed Upon Actions

2. *Management will establish an ongoing process that ensures:*
 - a. *Cardholder account information is routinely and accurately updated, and*
 - b. *Personal information is immediately removed from closed accounts and they are purged from the EAGLS online database after a reasonable period of time.*

Alternative Processes for Distribution of Sensitive Information Should Be Considered

OCAO and OCFO both maintain hardcopies of individual account information related to their office's responsibilities. Both offices ensure that the hardcopies are secured in locked cabinets or shredded. However, OCFO provides copies of individual travel billing statements to approving officials for review. Distribution of these billing statements poses a risk since they are sent through inner office mail in unsealed envelopes.

Security could be improved by providing the information to approving officials in electronic format; however, EAGLS does not provide these statements online for electronic distribution. FCA could create reports for approving officials by using BOA software to download the information. This would also reduce FCA's costs since FCA pays a fee for the hardcopies of the travel billing statements.

Another alternative would be for FCA to consider the availability of online billing statements when considering other companies for credit card services as recommended earlier in this report.

Agreed Upon Action

3. *FCA will improve control over sensitive information by using secure methods for disseminating any sensitive information.*