United States General Accounting Office

GAO

Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate

July 2002

MONEY LAUNDERING

Extent of Money Laundering through Credit Cards Is Unknown

GAO-02-670

Contents

Letter

1

Results in Brief 3
Background 6
The Extent to Which Credit Cards Are Used in Money Laundering Is Unclear 15
Industry Focus Is on Fraud and Credit Risk, Not Money Laundering 19
Regulatory Oversight for Anti–Money Laundering Requirements Is Not Focused on Credit Card Operations 28
Agency Comments and Our Evaluation 33

Appendixes

Appendix I: Scope and Methodology 35

Appendix II: Demographic Information about the Credit Card Issuers, Acquirers, and Processors in Our Review 37

Appendix III: Organizational Structure of the Associations in Our Review 40

Appendix IV: Observations on Money Laundering Scenarios 47

Appendix V: Review of SAR Database on Potential Money Laundering through Credit Cards 53

Tables

Table 1: Key Anti–Money Laundering Provisions and the Entities in the Credit Card Industry to Which They Apply 8
Table 2: Number and Dollar Value of Electronic Payments Transferred through U.S. Payment Systems in 2000 14
Table 3: Selected Characteristics of the Issuers in GAO's Review (Year Ending 2001) 37
Table 4: Selected Characteristics of Acquirers in GAO's Review (Year Ending 2001) 38
Table 5: Selected Characteristics of Credit Card Processors in GAO's Review (Year Ending 2001) 39

Figures

Figure 1: Money Laundering Stages 7
Figure 2: Typical Credit Card Transaction 13

Abbreviations

AML	Anti–Money Laundering
BSA	Bank Secrecy Act
CTR	Currency Transaction Report
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
NCCT	Non-Cooperative Countries and Territories
OFAC	Office of Foreign Assets Control
SAR	Suspicious Activity Report

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

July 22, 2002

The Honorable Carl Levin
Chairman, Permanent Subcommittee on Investigations
Committee on Governmental Affairs
United States Senate

Money laundering—the process of disguising or concealing illicit funds to make them appear legitimate—is a serious issue, with an estimated $500 billion laundered annually, according to the United Nations Office of Drug Control and Crime Prevention. The terrorist attacks of September 11, 2001, heightened concerns about money laundering and terrorist financing and prompted the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, (USA PATRIOT) Act of 2001 (the Patriot Act).[1] The goals of the Patriot Act include strengthening measures to prevent the supply of terrorist funding and strengthening the ability of the United States to prevent, detect, and prosecute international money laundering. As part of the subcommittee's efforts to combat money laundering, you asked us to review the vulnerabilities to money laundering that may exist in the credit card industry and the industry's efforts to address such vulnerabilities.

Money laundering has three stages: placement, where illicit cash is converted into monetary instruments or deposited into financial system accounts; layering, where the funds are moved to other financial institutions; and integration, where these funds are used to acquire assets or fund further activities. The credit card industry includes:

- credit card associations (associations), such as VISA and MasterCard, which license their member banks to issue bankcards, or authorize merchants to accept those cards, or both; [2]

- issuing banks, which solicit potential customers and issue the credit cards;

[1]Pub. L. 107-56, 115 Stat 272 (October 26, 2001). Title III of this act institutes new anti–money laundering requirements on all financial institutions and gives the U.S. Department of the Treasury the power to impose additional obligations on them as well.

[2]American Express and Discover Card were also included in our scope. They are not associations, but are full-service credit card companies that issue their own brand cards directly to customers and authorize merchants to accept their cards.

- acquiring banks, which process transactions for merchants that accept credit cards; and

- third-party processors, which contract with issuing or acquiring banks to provide transaction processing and other credit card–related services for the banks.

As agreed with your staff, the objectives of this report are to describe (1) vulnerabilities to money laundering that may exist in the credit card industry, (2) efforts by the industry to address potential vulnerabilities to money laundering using credit cards, and (3) existing regulatory mechanisms to oversee the credit card industry and help ensure the adequacy of required anti–money laundering (AML) programs.

In completing our review, we interviewed U.S. bank regulatory officials and representatives of the associations, major issuing and acquiring banks, and third-party processors. The credit card entities included in our review made up a significant portion of the U.S. credit card industry. From industry representatives, we requested documentation of existing AML programs—both broad AML programs and those specifically targeted for credit cards. However, only three institutions provided this documentation. The others described their AML programs but were unwilling to provide documentation to support their descriptions because of concern about the confidentiality of proprietary policies. Our summary of industry efforts was therefore based primarily on testimonial evidence. We also requested documentation from the credit card associations related to the reviews they conducted on offshore banks that were identified in a Senate Permanent Subcommittee on Investigations report on Correspondent Banking.[3] We received documentation from one association. The other association did not provide any documentation, citing, among other things, confidentiality laws in these offshore jurisdictions as a reason for not providing us with the documentation. They also told us that they could not locate the paperwork with respect to the reviews they conducted on these offshore banks.

[3]*Correspondent Banking: A Gateway to Money Laundering*, U.S. Senate Permanent Subcommittee on Investigations, Feb. 5, 2001.

We also interviewed law enforcement officials and asked the Financial Crimes Enforcement Network[4] (FinCEN) of the U.S. Department of the Treasury (Treasury) to analyze the government's database on Suspicious Activity Reports (SAR) and identify and quantify reports related to potential money laundering through credit cards. Appendix I contains more detailed information on the scope and methodology of our review. Appendix II provides detailed information on the entities in the industry that we interviewed.

Results in Brief

The extent to which money laundering through credit cards may be occurring is unknown. Bank regulators, credit card industry representatives, and law enforcement officials we interviewed generally agreed that credit card accounts were not likely to be used in the initial stage of money laundering when illicit cash is first placed into the financial system, because the industry generally restricts cash payments. Bank regulators and credit card industry representatives we interviewed acknowledged that credit card accounts might be used in the layering or integration stages of money laundering. For example, by using illicit funds already placed in a bank account to pay a credit card bill for goods purchased, a money launderer has integrated his illicit funds into the financial system. Most law enforcement officials we met with were unable to cite any specific cases of credit card–facilitated money laundering in U.S.–based financial institutions. Further, a FinCEN analysis of its database of SARs filed by U.S.-based financial institutions revealed very little evidence of potential money laundering through credit cards. However, evidence from a congressional investigation showed that credit card accounts accessed through banks in certain offshore financial secrecy jurisdictions[5] could be vulnerable to money laundering. In addition to the

[4]FinCEN was established in 1990 to support law enforcement agencies by analyzing and coordinating financial intelligence information to combat money laundering. The agency is also responsible for promulgating regulations under certain provisions of the Bank Secrecy Act.

[5]The Internal Revenue Service defines financial secrecy jurisdictions as jurisdictions that have a low or zero rate of tax, a certain level of banking or commercial secrecy, and relatively simple requirements for licensing and regulating banks and other business entities. In this report, we use the term "offshore jurisdictions" to refer to financial secrecy jurisdictions.

cases described in the Permanent Subcommittee's February 2001 report,[6] the Internal Revenue Service's Criminal Investigation group has investigated cases of U.S. citizens placing funds in bank accounts in these jurisdictions in order to evade U.S. taxes and accessing the funds through the use of credit cards.

Industry representatives generally reported that they did not have AML policies and programs focused on credit cards because they considered money laundering using credit cards to be unlikely. In their view, the banks' application screening processes, systems to monitor fraud, and policies restricting cash payments and prepayments[7] made credit cards less vulnerable to money laundering. Industry representatives also described policies and programs to minimize financial risks of credit card fraud, which they believed to be helpful in detecting money laundering. For example, the major associations told us that they monitor card transactions for potential fraud and report the results of their monitoring to member banks, which may use the information to investigate and report activities that the banks consider suspicious. Association officials also told us they applied the same due diligence procedures for domestic and foreign issuing and acquiring banks. At the time of our review, this due diligence did not include anti-money laundering screening**.** Credit card–issuing and –acquiring institutions told us that they screen applications and monitor transactions through automated systems for unusual or out-of-pattern transactions and, as a result of these efforts, may conduct investigations, file SARs, or work with law enforcement. The major third-party credit card processors in our study told us that they incorporated fraud prevention and detection policies and programs into their transaction processing systems for the issuers and acquirers. Although most of the industry representatives indicated that their fraud controls might also identify money laundering, they were unable to cite any cases of money laundering identified as a result of their fraud controls. The lack of money laundering cases identified through these fraud controls and the lack of indications of money laundering through suspicious activity reporting might be attributed to such factors as a lack of money laundering occurring through U.S.-based credit card operations or the inadequacy of current fraud-focused procedures and systems to identify money laundering. Treasury believes

[6]*Correspondent Banking: A Gateway to Money Laundering*, U.S. Senate Permanent Subcommittee on Investigations, Feb. 5, 2001.

[7]A prepayment is a payment made to a credit card account in an amount that exceeds the total balance of the account and can result in a large overpayment.

that the systems the industry uses to monitor fraud are a starting point for appropriate anti–money laundering safeguards, but alone they are not sufficient. Treasury believes that while AML programs should be built upon existing anti-fraud programs, additional factors and considerations specific to money laundering must be included.

At the time of our review, the primary regulatory oversight mechanism to help ensure the adequacy of AML programs was the Bank Secrecy Act (BSA) examination, which applied, in the credit card industry, to issuing and acquiring banks. The regulators told us that, in their view, the issuing banks' application screening process, fraud monitoring systems, and policies generally restricting cash payments lowered the risk of money laundering through credit cards. Consequently, regulators focused less on credit card operations in conducting their BSA examination than on other areas that they considered at higher risk to money laundering, such as private banking and wire transfers. Although acquiring banks are subject to the BSA, the regulatory oversight of these entities has focused more on safety and soundness issues because regulators do not view these entities as being at high risk for money laundering. The associations and third-party processors are currently subject to regulatory oversight solely focused on the data processing systems and internal controls of these entities, to ensure that these entities do not pose risks to the banks they service. The Patriot Act required the associations to have AML programs by April 24, 2002.[8] Interim final rules issued by Treasury on April 24, 2002, require the associations' anti–money laundering program to be in writing, approved by senior management, and to be reasonably designed to prevent the credit card system from being used to launder money or to finance terrorist activities. Under BSA regulations, the Internal Revenue Service is the regulatory body that will oversee the associations' adherence to the new requirements, unless Treasury delegates this authority to another agency.

We make no recommendations in this report. We asked Treasury and two of its bureaus, the Office of the Comptroller of the Currency and FinCEN, to comment on this report. We also asked the Board of Governors of the

[8]Section 352 (a) of the Patriot Act amends section 5318(h) of the BSA. As amended, section 5318(h)(1) of the BSA requires every financial institution to establish an anti–money laundering program. As operators of credit card systems are identified as financial institutions under the BSA, 31 U.S.C. § 5312(a)(2)(L), they are subject to the anti–money laundering program requirements. Treasury, in its interim final rule, defined an operator of a credit card system. This definition includes credit card associations as operators of a credit card system.

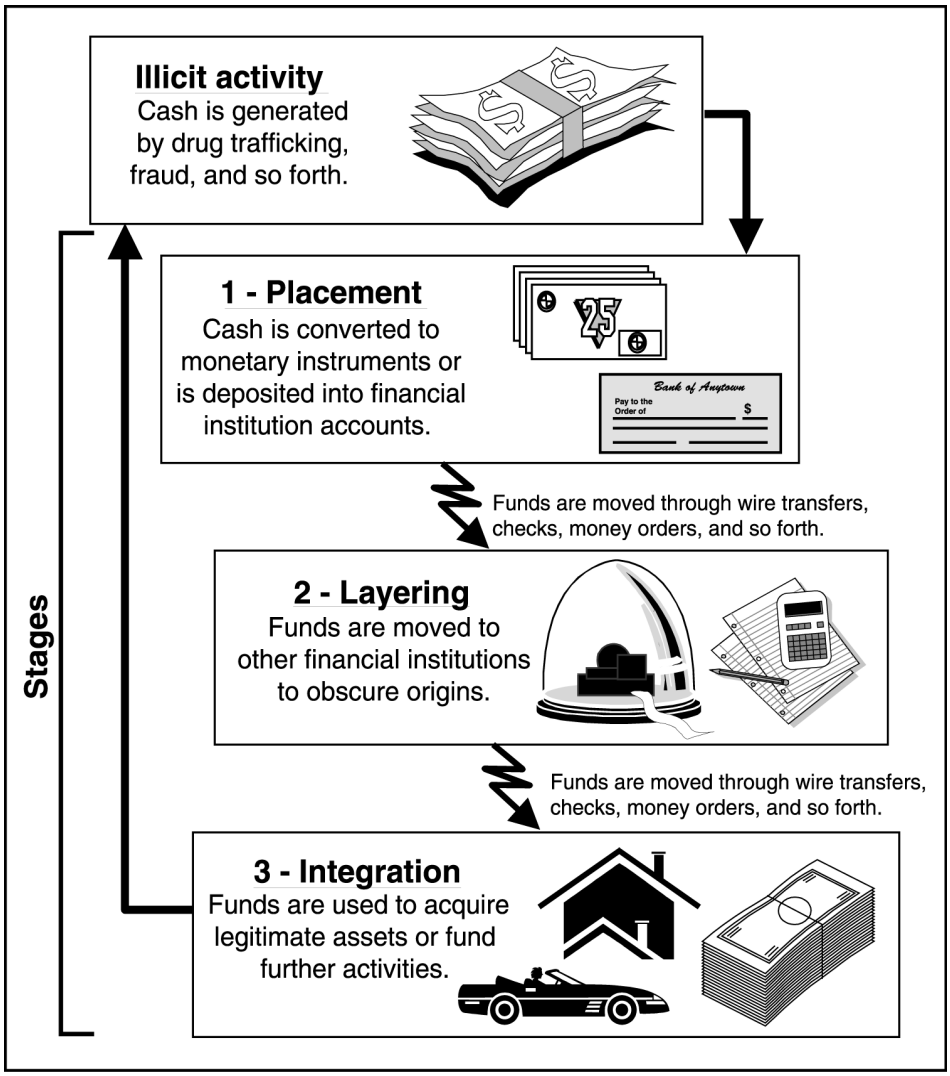
Federal Reserve System and the Federal Deposit Insurance Corporation for their comments on it. The agencies generally agreed with the information presented in the report and provided us with technical changes or factual updates, which we have incorporated where appropriate.

Background

Individuals engaged in illicit activities must eventually introduce their illegally gained money into the nation's legitimate financial systems, according to FinCEN. Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Through money laundering, the criminal transforms the monetary proceeds derived from criminal activity into funds with an apparently legal source. Money laundering provides the fuel for drug dealers, terrorists, arms dealers, and other criminals to operate and expand their criminal enterprises. FinCEN notes that criminals are able to use financial systems in the United States and abroad to further a wide range of illicit activities.

Money laundering generally occurs in three stages, as shown in figure 1. In the first, or placement, stage, cash is converted into monetary instruments, such as money orders or travelers' checks, or deposited into financial institution accounts. The later stages of money laundering are the layering and integration stages. In the layering stage, the funds already placed are transferred or moved into other accounts or other financial institutions to further obscure their illicit origin. In the integration stage, the funds are used to purchase assets in the legitimate economy or to fund further activities.

Figure 1: Money Laundering Stages



Source: *FinCEN Related Series: An Assessment of Narcotics Related Money Laundering*, FinCEN, July 1992.

AML Requirements for the Credit Card Industry

AML requirements for financial institutions focus on mandating that the financial institutions keep records and file reports for certain types of transactions and establish programs to prevent and detect money laundering.[9] Table 1 shows some of the key anti–money laundering requirements and the entities in the credit card industry to which they apply.

Table 1: Key Anti–Money Laundering Provisions and the Entities in the Credit Card Industry to Which They Apply

Statute and regulations	Some key provisions	Associations	Issuing banks	Acquiring banks
1970 Bank Secrecy Act (31 U.S.C. § 5313)	BSA authorizes Treasury to promulgate regulations for transactions in currency.	X	X	X
31 C.F.R. § 103.22	Requires reports to FinCEN of receipts or transfers of U.S. currency in excess of $10,000 using the Currency Transaction Report (CTR). Also requires reporting of all known receipts or transfers by one entity that exceed $10,000 in 1 day.[a]		X	X
31 U.S.C. § 5331 & 31 C.F.R. §103.30	Requires the reporting of cash transactions over $10,000 on Form 8300.	X		
Money Laundering Control Act of 1986 (18 U.S.C. § 1956 and 1957)	Makes it a criminal offense to knowingly engage in financial transactions that involve profits from certain illegal activities.	X	X	X
1992 Annunzio-Wylie Money Laundering Act (31 U.S.C. § 5318(h))	Gives the Secretary of the Treasury authority to promulgate regulations requiring financial institutions to establish AML programs.	X	X	X

[9]Financial institutions cannot issue or sell bank checks and drafts, cashiers' checks, money orders, or travelers' checks for $3,000 or more in currency without recording certain information and verifying the identity of the purchaser. 31 C.F.R. § 103.29(a) (2001). Additionally, each financial institution must retain for a period of 5 years the records of certain transactions that exceed $10,000, including records of each extension of credit in an amount that is greater than $10,000. 31 C.F.R. § 103.33 (2001).

(Continued From Previous Page)

Statute and regulations	Some key provisions	Associations	Issuing banks	Acquiring banks
1992 Annunzio-Wylie Money Laundering Act (31 U.S.C. § 5318(g))	Amends the BSA and authorizes the Treasury to require any financial institution and its officers, directors, employees, and agents "to report any suspicious transaction relevant to possible violation of law or regulation."	X	X	X
1996, Suspicious Activity Reporting Rule for banks and other depository institutions, 31 C.F.R. § 103.22	Requires banks and other depository institutions to report suspicious activities for transactions involving $5,000 or more to FinCEN. [a]		X	X
October 26, 2001, U.S. Patriot Act, Section 326	Requires Treasury to issue regulations, effective October 26, 2002, to establish minimum procedures for financial institutions to use in verifying the identity of a customer during the account opening process.	X	X	X
October 26, 2001, U.S. Patriot Act, Section 352	Requires financial institutions to establish anti–money laundering programs by April 24, 2002, that address: (i) the development of internal policies, procedures, and controls; (ii) the designation of a compliance officer; (iii) an ongoing employee training program; and (iv) an independent audit function to test this program.	X	X	X
April 24, 2002, Financial Crimes Enforcement Network; Anti–Money Laundering Programs for Operators of a Credit Card System	Defines operator of a credit card system and requires each operator to have a written anti–money laundering program with certain minimum standards by July 24, 2002. The program must be approved by senior management and reasonably designed to prevent the system from being used to launder money or finance terrorist activities.	X		
October 26, 2001, U.S. Patriot Act, Section 313	Bars (as of December 25, 2001) certain financial institutions from maintaining correspondent bank accounts for foreign shell banks (that is, a bank that does not have a physical presence in any country). [b]		X	X

[a]Regulations concerning currency transaction reports and suspicious activity reports are not applicable to associations.

[b]An insured bank, a commercial bank, a private banker, an agency or branch of a foreign bank in the United States, an insured institution as defined in 12 U.S.C. § 1724(a), a thrift, or broker/dealer.

Source: BSA, BSA Regulations, and the Patriot Act.

Financial institutions are also required to abide by regulations developed by the Office of Foreign Assets Control (OFAC). OFAC, which is a division of Treasury, administers and enforces economic and trade sanctions against targeted foreign countries, terrorism-sponsoring organizations, and international narcotics traffickers. On the basis of U.S. foreign policy and national security goals, OFAC promulgates regulations and develops and

administers sanctions for Treasury under eight statutes. In general, financial institutions are required when so instructed by OFAC to block the accounts and other assets of specified countries, entities, and individuals. OFAC has authority to impose civil penalties when financial institutions fail to comply.

Financial institutions are also advised by regulators to enhance their scrutiny of certain transactions and banking relationships in jurisdictions deemed by FinCEN to have serious deficiencies in their anti–money laundering systems. The jurisdictions identified by FinCEN are consistent with the Financial Action Task Force's (FATF)[10] list of Non-Cooperative Countries and Territories (NCCT).[11]

Federal banking regulators examine banks to determine whether their policies, procedures, and internal controls are adequate with respect to BSA, AML, and OFAC laws and regulations. The regulators generally are required to take the following steps in assessing the banks:

- Determine whether bank management has adopted and implemented adequate policies and procedures related to BSA, AML, and OFAC. These policies are expected to address the identification and reporting of money laundering in its different forms (that is, placement, layering, and integration).

- Ensure that these policies cover all products and units in the bank, including credit cards.

- Verify that the bank's board has approved a written compliance program that ensures compliance with all reporting and record-keeping requirements of the BSA, including SAR requirements. This includes

[10]The FATF, with 28 member countries, is an intergovernmental body established in 1989 to promote policies to combat money laundering. In 1990, FATF issued an initial report containing 40 recommendations for fighting money laundering.

[11]In 1999–2000, FATF began a process to identify jurisdictions with serious deficiencies in anti–money laundering regimes. As a result, FATF published a report in June 2000 listing 15 jurisdictions with serious deficiencies in their anti–money laundering efforts. These jurisdictions were placed on the NCCT list of the FATF. FATF published additional reports in June and September 2001 that resulted in the removal of four countries from NCCT status and the addition of eight new NCCTs. As of this writing, there are 19 countries designated by FATF as NCCTs. FATF calls on its members to request that their financial institutions give special attention to businesses and to transactions with persons in countries identified as being noncooperative when these businesses or persons do not rectify the situation.

independent testing for compliance, designation of a qualified individual or individuals for coordinating and monitoring day-to-day compliance, and training for appropriate personnel.

- Determine the effectiveness of the bank's processes in identifying risk. The regulators expect that banks will conduct a risk assessment of their customer base to determine the appropriate level of necessary due diligence. The regulators also determine whether a bank 1) has filed the required BSA reports; 2) has maintained the required BSA records; 3) can detect structuring; and 4) has an effective overall system to monitor, identify, review, and report suspicious activity.

The Credit Card Industry Is Composed of Various Entities

The credit card industry is composed of the following four types of entities:

- Associations, which are jointly owned by member financial institutions, provide the computer systems that transfer data between member institutions. The associations also establish the operating standards that define the policies, roles, and responsibilities of their member institutions. Most member institutions issue credit cards, or sign up merchants to accept credit cards, or both. Providing direct services to consumers and merchants is the responsibility of the member institutions rather than of the associations. The major associations are VISA and MasterCard. Appendix III provides more information on the organizational structure of VISA and MasterCard. Although not an association, American Express has arrangements in some overseas markets for licensing foreign banks to issue American Express cards. This creates relationships similar to those that VISA and MasterCard have with their issuing card member banks.

- Issuing banks solicit potential customers and issue the credit cards. These banks carry the credit card loan and set policies for matters such as credit limits for cardholders and treatment of delinquent cardholders. These banks maintain all account information on the cardholder. In many respects, American Express and Discover Card act as issuing banks. That is, they issue their own brand cards. They also sign up the cardholder, settle the transactions, and maintain all account information on the cardholder.

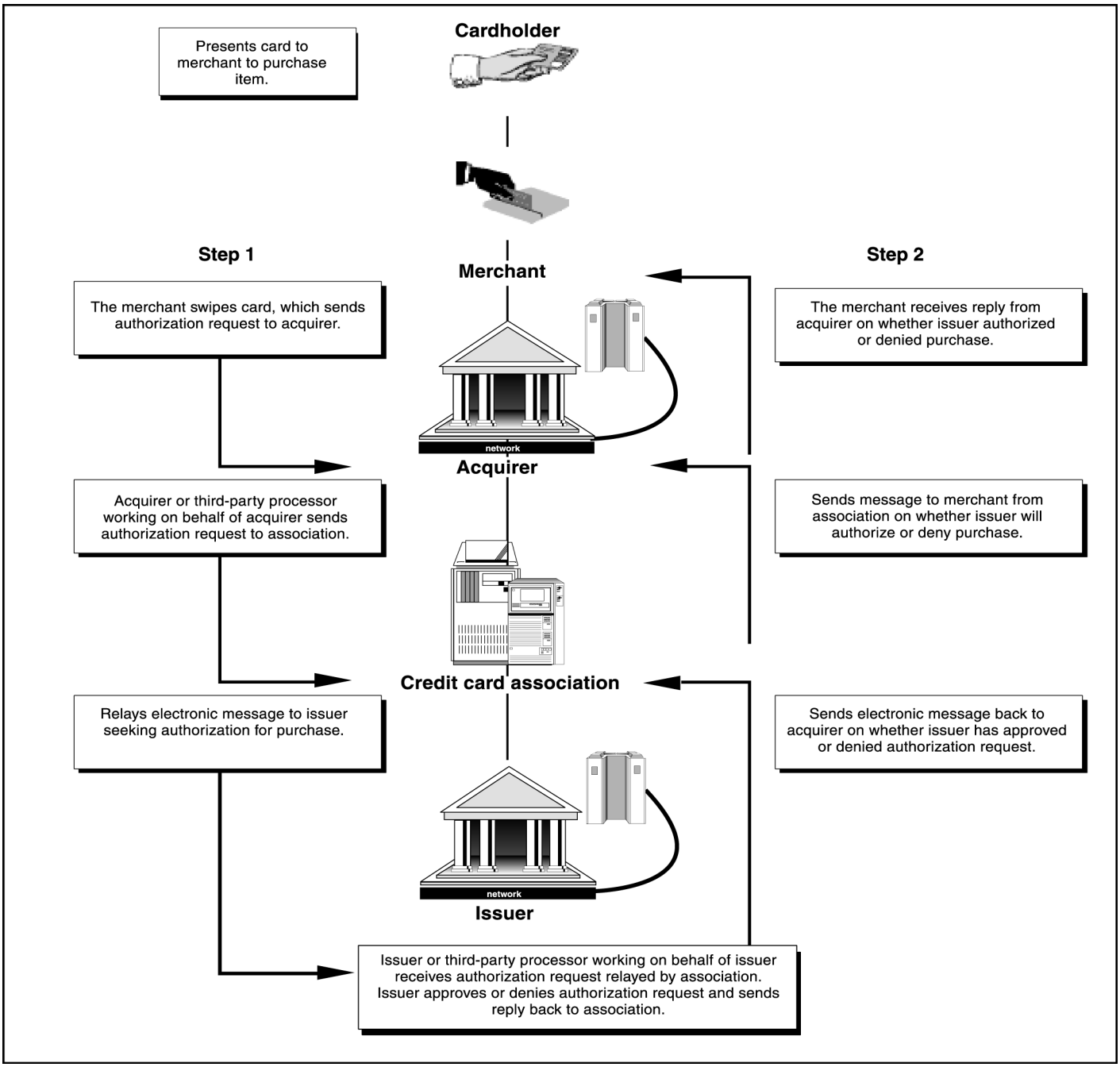
- Acquiring banks, also known as merchant banks, sign up merchants to accept credit cards. These banks settle the credit card transactions and maintain all account information on their merchant clients. American

Express and Discover Card also perform many merchant bank functions. For the most part, they sign up merchants directly, settle accounts, and maintain all account information on their merchants.

- Third-party credit card processors process credit card transactions for the issuing or acquiring banks that contract with them to perform these services. These processors also perform a range of other functions for issuing and acquiring banks, including embossing cards for issuing banks or soliciting merchants for acquiring banks. Third-party processors are usually able to perform these functions for issuing or acquiring banks at lower cost than the banks because they have reached economies of scale. A specialized group of third-party processors, known as independent sales organizations, mainly solicit merchants on behalf of acquiring banks.

Each of the various types of entities plays a role in each credit card transaction, as shown in figure 2.

Figure 2: Typical Credit Card Transaction



Source: VISA.

Average Dollar Value of Credit Card Transactions Very Small Compared with Other Forms of U.S. Electronic Payments

In 2000, the credit card industry processed a large number of relatively small, average dollar–value transactions as compared with other forms of electronic payments, as shown in table 2. During the year, 20 billion of the 72.5 billion (28 percent) electronic payments transferred through U.S. payment systems were made up of credit card transactions. However, the average dollar value of credit card transactions was very small as compared with other forms of electronic payments. For example, the average value of a credit card transaction was $70, which was very small as compared with the average value of transactions for other forms of electronic payments, such as Fedwire and the Clearinghouse Interbank Payment System, which were $3.5 million and $4.9 million, respectively.

Table 2: Number and Dollar Value of Electronic Payments Transferred through U.S. Payment Systems in 2000

		Daily average		Annual		
System	**Purpose**	**Number**	**Dollar value**	**Number**	**Dollar value**	**Average value of transaction**
Fedwire	Funds transfer operated by Federal Reserve System, used primarily for domestic payments between financial institutions.	430,000	$1.5 trillion	108 million	$380 trillion	$3.5 million
Clearing House Interbank Payment System (CHIPS)	Privately owned large dollar value payments transfer system used primarily for settling foreign exchange transactions.	237,000	1.2 trillion	60 million	292 trillion	4.9 million
Automated Clearing House (ACH)	Systems operated by the Federal Reserve System and private organizations to transmit electronic payments for retail purposes.	120 million[b]	28 billion[b]	30 billion	7 trillion	233
Automated Teller Machines	Cash dispensing and account fund transfers.	52 million[b]	3.2 billion[b]	13 billion	800 billion	62
Credit cards	Payments for goods and services through third-party financial institutions.	80 million[b]	5.6 billion[b]	20 billion	1.4 trillion	70
Debit cards[a]	Payments for goods and services directly from payor's financial institution.	37 million[b]	1.6 billion[b]	9.3 billion	400 billion	43
Total		**290 million**	**$2.74 trillion**	**72.5 billion**	**$682 trillion**	

[a]Includes both on-line and off-line transactions.

[b]Estimated from annual data by assuming 250 business days per year.

Source: Federal Reserve Board of Governors, New York Clearing House, and National Automated Clearing House Association.

The Extent to Which Credit Cards Are Used in Money Laundering Is Unclear

The consensus from industry, bank regulatory, and law enforcement officials we interviewed was that credit card accounts were not likely to be used in the initial stage of money laundering when illicit cash is first placed in the financial system, primarily because of restrictions on cash payments. Some credit card industry representatives and bank regulators we interviewed acknowledged that credit cards could be used in the layering or integration stages of money laundering; however, the extent to which this may be occurring is unknown. These officials, as well as most law enforcement officials we spoke with, were not aware of any cases of money laundering through credit cards in U.S.-based institutions. An analysis of FinCEN's SAR database also did not identify any instances in which the suspicious activity reported by financial institutions developed into an actual case of money laundering. However, we received information from one law enforcement agency that individuals have used credit cards to access illicit funds held in banks or trusts established in certain offshore jurisdictions.

Credit Cards Are Unlikely to Be Used in Placement Stage, but Their Use in the Later Stages of Money Laundering Is Unknown

Credit cards are not likely to be used to place illicit funds in the U.S. financial system because of restrictions on cash payments, according to industry, bank regulatory, and law enforcement officials we interviewed. For example, most issuers and acquirers told us that they did not accept cash payments for credit card accounts and generally restricted payments to checks. Some industry and regulatory officials indicated that credit cards would be an ineffective way to launder money because each transaction creates a paper trail. They also indicated that credit cards would be an inefficient way to launder funds because of the limits on access to cash.

Nevertheless, some of these officials acknowledged that credit cards could be used at the layering and integration stages of money laundering; however, the extent to which this may be occurring is unknown. They indicated that once money launderers had placed their illicit funds in the financial system, they could layer and integrate the funds using credit card accounts. These officials provided us with examples of how this could occur:

- The money launderer prepays his credit card using funds already in the banking system, creating a credit balance on the account. The launderer then requests a credit refund, which enables him to further obscure the origin of the funds, which is layering.

- The money launderer uses the illicit funds that are already in the banking system to pay his credit card bill for goods purchased, which is an example of integration.

Officials from one bank told us that once its bank receives a check payment for a credit card account, it has no way of knowing how the funds were put into the system, let alone the origin of funds. Officials from another bank stated that if a money launderer were able to deposit funds into another institution, they could easily obtain a credit card. Appendix IV contains information on six money-laundering scenarios that we discussed with industry and regulatory officials.

Although industry and regulatory officials acknowledged that credit cards could be used in the layering or integration stages of money laundering, they, along with most law enforcement officials we interviewed, were unaware of actual cases in which credit cards were used to launder money through U.S.-based financial institutions. An analysis of FinCEN's database of SARs filed by U.S.-based financial institutions also did not identify any instances in which the suspicious activity reported by the financial institution developed into actual cases, but it provided some insights about possible money laundering linked to the use of credit cards. The database analysis FinCEN conducted in response to our request found that some banks had filed SARs pertaining to possible money laundering/BSA/structuring violations and credit, debit,[12] or ATM cards.[13] FinCEN conducted an analysis of the database and found that between October 1, 1999, and September 30, 2001, banks had filed 499 SARs related to credit, debit, or ATM cards and potential money laundering. This represents a significantly small percentage of the total of all SARs filed in this period: about one-tenth of 1 percent. FinCEN's analysis identified some examples of the type of suspicious activity banks reported that related to the layering and integration stages of money laundering:

[12]A debit card is a plastic card that is tied directly to an individual's checking or savings account. The debit card has the logo of one of the major associations, allowing the individual to make a purchase with the card from merchants who accept the association's credit cards. Transactions from debit cards are quickly deducted from the individual's checking or savings account, which differs from a credit card transaction, which the individual pays at a later date.

[13]The ATM card is a plastic card that, like the debit card, is tied directly to an individual's checking or savings account. It can be considered a debit card if it contains the logo of a major association. The ATM card is used to conduct banking business at an Automatic Teller Machine, such as depositing or withdrawing funds or checking on account balances.

- Fifteen of the 499 SARs related to customers overpaying their credit cards and subsequently asking for refund checks. FinCEN noted that overpaying a credit card could be used as a means to launder money because it provides a simple means to convert criminal or suspicious funds to a bank instrument with minimal or no questions as to the origin of the funds.

- One hundred fifteen of the 499 SARs related to customers trying to structure deposits—that is, making multiple deposits below the $10,000 threshold that would trigger a bank's filing a Currency Transaction Report (CTR). Most of these SARs related to cash transactions wherein the customer asked to deposit funds into various accounts, pay down loans, purchase cashiers' checks, and make credit card payments. FinCEN noted that the total payments on the credit cards were typically well over $5,000 and often exceeded $10,000.

FinCEN noted that the activity reported in virtually all of the SARs was considered "an isolated incidence" by the reporting banks. The only exception involved six SARs filed in early 2001 by the same bank, which reflects some kind of organized or criminal activity involving credit cards. Specifically, this bank filed SARs on four suspects. The bank reported that check payments credited to the four suspects' credit card accounts were made by a fifth individual. The individual making the payments on these accounts had earlier been indicted on money laundering, contraband, cigarette smuggling, and visa/immigration fraud charges.

Of the 499 SARs that FinCEN identified, 70 were referred directly to law enforcement by the financial institution, in addition to being filed with FinCEN. FinCEN was unable to tell us if any of them resulted in money laundering cases. Appendix V contains more details on the FinCEN analysis of the SAR database.

Credit Card–Accessed Accounts in Offshore Banks Create Vulnerabilities to Money Laundering

One U.S. law enforcement agency has found instances of the use of credit cards associated with bank accounts in offshore jurisdictions to launder money, but the extent of this activity is unknown. For example, the Internal Revenue Service's Criminal Investigation group has found that U.S. citizens have placed funds intended to evade U.S. taxes in accounts at banks or trusts in certain offshore jurisdictions and then accessed these funds using credit and debit cards associated with the offshore account. In other instances, individuals generating cash from illegal activities have smuggled the cash out of the United States into an offshore jurisdiction with lax regulatory oversight, placed the cash in offshore banks, and—again—accessed the illicit funds using credit or debit cards. The credit or debit card provides a money launderer access to the cash received through the criminal activity without having to be concerned about a CTR or SAR being filed, according to this law enforcement agency. A United Nations report on offshore jurisdictions[14] reported that credit cards are a common and nontraceable means by which individuals access their funds in these offshore jurisdictions. The report indicated that banks assure cardholders that their account information will be protected by strict bank secrecy laws in these jurisdictions.

The Senate Permanent Subcommittee on Investigations report on Correspondent Banking describes two cases in which offshore banks engaged in money laundering, provided their clients with credit or debit cards to access their illicit funds. Guardian Bank and Trust (Cayman) Ltd., was an offshore bank licensed in the Cayman Islands. Its owner, who pleaded guilty to money laundering, tax evasion, and fraud, described how the bank allowed U.S. citizens to establish accounts with the bank for the purpose of evading taxes. The owner promoted the use of credit or debit cards so that his clients could covertly access funds stored in the Cayman Islands. He stated that these techniques were promoted and used to evade U.S. taxation. Caribbean American Bank, which was licensed in Antigua and Barbuda, was involved in a major fraud scheme. Through its relationship with another bank, it was able to offer its clients credit cards to charge purchases. The balance on the card was paid out of the illicit proceeds the clients had on deposit at Caribbean American Bank.

[14]*Financial Havens, Banking Secrecy and Money Laundering*, United Nations Office for Drug Control and Crime Prevention, Global Programme Against Money Laundering, May 29, 1998.

Industry Focus Is on Fraud and Credit Risk, Not Money Laundering

Industry representatives of most of the entities we reviewed told us that they did not have AML policies and programs specifically focused on the issuance and use of credit cards because they considered money laundering through the use of credit cards to be unlikely. They indicated that issuing and acquiring banks' application screening processes, systems to monitor fraud, and policies restricting cash payments and prepayments made credit cards less vulnerable to money laundering. The credit card industry had a variety of policies and programs aimed at reducing the industry's losses from fraud and credit risk, which are the major financial risks in the credit card industry.[15] For example, credit card–issuing and –acquiring institutions told us that they screen applications and monitor transactions through automated systems for unusual or out-of-pattern transactions and, as a result of these efforts, may conduct investigations, file SARs, or work with law enforcement. Industry representatives and some regulatory and law enforcement officials we interviewed believed these policies and programs could also help identify possible money laundering through credit cards; however, none of them had evidence that the fraud systems identified money laundering. The lack of evidence of money laundering identified through the fraud systems could be attributed to such factors as a lack of money laundering occurring through U.S.-based credit card operations or the inadequacy of current fraud-focused procedures and systems to identify money laundering. Treasury believes that the systems the industry used to monitor fraud are a good starting point for AML safeguards, but the industry must also include additional factors and considerations specific to money laundering.

Credit Card Associations Are Required to Have Anti–Money Laundering Programs as a Result of the Patriot Act

The associations' approaches to addressing AML issues have changed significantly as a result of the Patriot Act, according to association officials. At the start of our review, the provisions of the Patriot Act requiring all financial institutions to have AML programs in place were not yet in effect, and Treasury had not issued regulations requiring credit card associations to have in place AML policies and programs. Representatives of the two major credit card associations we interviewed at that time did not view credit cards as being at high risk for money laundering. They also did not

[15]Fraud results in financial losses to the industry and can take the form of stolen or counterfeit credit cards as well as merchants engaging in fraudulent activity. Credit risk also results in financial losses to the industry when, for example, cardholders do not pay their credit card bills or merchants declare bankruptcy and are unable to cover their outstanding charges.

regard the establishment of AML policies and programs as the responsibility of their respective associations. Nevertheless, the association officials believed that their due diligence procedures for membership in the associations for domestic and foreign issuing and acquiring banks, as well as their fraud controls, were useful in identifying suspicious activity. Officials from one of the associations indicated that its fraud controls could possibly identify money laundering, while officials from the other association indicated that its fraud controls were developed strictly to identify fraud, not money laundering. Treasury acknowledges that the associations' fraud monitoring is sophisticated but is not convinced that it can easily detect money laundering.

The association officials told us that they generally applied the same due diligence procedures for domestic and foreign issuing and acquiring banks. These procedures included:

- obtaining documentation showing that the bank is licensed and subject to bank supervision and regulation in the jurisdiction where it is licensed;

- applying underwriting procedures to ensure that the bank is financially sound and can meet its financial obligations; and

- obtaining assurances that the bank will abide by the association's rules and regulations and comply with applicable host country laws.

The association officials told us that the associations did not apply separate due diligence procedures to verify the AML policies and programs of their domestic and foreign issuing and acquiring banks, including banks in NCCT countries. Association officials told us that they relied on host country regulators to ensure that issuing and acquiring banks were not engaged in money laundering activity. As discussed below, the associations' due diligence procedures for reviewing their member banks' AML programs will change as a result of the Patriot Act.

Association officials told us that although the associations did not have formal AML policies or programs before the Patriot Act, they have had longstanding in-house systems to monitor abnormal or unusual card transactions in terms of dollar amounts, locations of purchases, and frequency of charges. The associations monitor these transactions as they pass through the associations' networks and related fraud screens. The monitoring systems have helped member banks, some of which must be

subscribers to the associations' fraud services, to identify and investigate suspicious activity. The associations reported the results of this monitoring to member banks and, if requested by member banks, have helped them report cases of fraud to the appropriate law enforcement agencies. Officials of one of the associations indicated that this monitoring may also help identify possible money laundering, but they could not cite any cases where money laundering had been identified by their monitoring system.

The Patriot Act required the associations to have AML programs by April 24, 2002. Treasury has promulgated interim final rules to provide guidance to associations concerning the requirements for the AML programs. Treasury requires that by July 24, 2002, associations have AML programs with certain specified minimum standards. More specifically, associations are required to have policies, procedures, and controls to mitigate the risk for money laundering and terrorist financing; these policies, procedures, and controls are to be focused on the process of authorizing and maintaining authorization for issuing and acquiring banks. Treasury expects the associations to focus their efforts on those banks considered as being at high risk for money laundering. For example, Treasury considers offshore banks in jurisdictions with lax money laundering controls to be high-risk entities.

We met with officials of the associations after the enactment of the Patriot Act. At that time, officials of one of the associations told us that as part of their effort to meet the goals of the Patriot Act, they were augmenting their procedures for reviewing all of their member banks to ensure that the association was not at risk for being used for money laundering by one of its member banks. The officials indicated that they would review their entire member base but focus on those members in jurisdictions that are considered to be at high risk for money laundering. For example, they would first focus their efforts on those jurisdictions identified as NCCT by the FATF. Officials from the other association did not provide us with any descriptions of how they might change their procedures for reviewing their member banks, and indicated that they were waiting for Treasury to provide guidance on how they should review these banks. These officials indicated, however, that they would be in compliance with the Patriot Act by the required dates.

Issuers Believe Fraud-Focused Policies and Controls and Restrictions on Cash and Prepayments May Help Counter Money Laundering

In the view of the issuers we interviewed, their fraud-focused policies and controls, as well as their restrictions on cash payments and prepayments, can serve to help prevent and detect money laundering via credit cards. However, Treasury believes that while these fraud-focused policies and controls are a starting point for appropriate anti–money laundering safeguards, the industry must also consider additional factors and considerations specific to money laundering. Most of the issuers we spoke with had broad AML programs, but only three of the nine in our review had AML policies and programs specifically addressing credit card operations. Nevertheless, all of the issuers told us that they applied fraud and credit risk policies and controls to screen credit card applications and monitored the card transactions of approved cardholders. In addition, issuers told us that they placed restrictions on cash and prepayment transactions.

The issuers told us that they had application screening procedures to authenticate the applicant and review the applicant for purposes of identifying potential fraud. The issuers said that they authenticate applicants by verifying employment, address, social security number, or other application information against external sources such as public, credit bureau, or employer records. To review the applicant for potential fraud, some issuers said that they try to match the applicant's name and other identifying information against names and information on public records and industry lists, or "negative lists"—lists containing names and addresses associated with fraudulent activity. Three issuers also said that they declined to process applications with foreign addresses. Most of the issuers, furthermore, told us that they matched the applicant's name and address against the OFAC list of prohibited individuals or entities. The issuers believe that their application screening process, as a whole, enables them to identify and reject applicants who have been associated with fraudulent activity or show a potential for fraud or other criminal activity, including money laundering. However, since the issuers rely on public records or lists of names and addresses known for fraud, the issuers' screening process may not capture all fraudulent or criminal activity. For example, applicants who have no negative credit or criminal history would be able to avoid scrutiny and detection under their screening process, according to the issuers.

The issuers told us that they also monitor the card transactions of approved cardholders for fraud and changes in credit status. The issuers believed that their automated monitoring aids in reducing the risk of fraud or potential cases of money laundering via credit cards; however, they were unable to cite any cases of money laundering identified as a result of their fraud controls. The issuers used fraud risk scoring models[16] to monitor transactions by frequency, type, dollar size, and location and determine whether the transaction is unusual, out of pattern, or potentially fraudulent. Several of the issuers said that if their automated monitoring identifies card transactions that significantly deviate from a cardholder's expected spending pattern, the transaction is flagged and their system alerts them, giving them the flexibility to exercise several options. These options include:

- denying authorization for the credit purchase;
- concluding that the transaction is suspicious and investigating it;
- cuing the issuer's system to collect additional information;
- filing a SAR about the transaction to FinCEN and, if urgent, notifying law enforcement directly;
- canceling the cardholder's account; and
- referring the cardholder's name to an industry negative list.

Issuers indicated that they defer to law enforcement to determine whether their reports of suspicious activities involve money laundering.

With respect to prepayments, issuers said they monitor prepayments and the large credit balances that prepayments generate. Some issuers asserted that their monitoring effort creates a "transaction trail" that exposes possible money launderers and money laundering activities, and thereby makes credit cards a tool disfavored by money launderers.

[16]Fraud or risk scoring is a technique that scores the transactions of cardholders, on a real-time basis, to identify potentially fraudulent or financially risky patterns. A common type of scoring model used by the issuers in our review involved the use of predictive software, based on neural network technology.

The issuers varied in how they monitored prepayments and credit balances. For example, a few said that they flagged and tracked all credit balances. Others said that they tracked them by size of prepayment, giving more scrutiny to large prepayments in terms of absolute dollars or as a proportion of a customer's credit line. Other characteristics that issuers said they tracked include credit balance size and discernable suspicious pattern. The issuers also stated that they limited the amounts that a cardholder carrying a credit balance could withdraw from the card, and they monitored the reduction of credit balances by type and location of reductions. For example, when the cardholder wished to reduce the credit balance by obtaining cash advances, quasi-cash (such as gambling chips), or credit purchases, the issuers monitored these transactions and limited the amounts the cardholder could access.

Several of the issuers further stated that if cardholders with large credit balances asked for refunds, the issuers tracked these transactions and did not automatically give the refunds. Some issuers told us that they first reviewed or investigated the request for a refund, or required the cardholder to submit a written request for the refund, as provided by Regulation Z.[17] For example, an issuer told us that in mid-September 2001, their system flagged a large credit balance, and the cardholder, who was staying at a major hotel in Boston, requested an immediate refund through wire transfer to a checking account. The cardholder reportedly wanted to leave the United States and travel via private plane to a Middle Eastern country. The issuer told us that it initially denied the refund after explaining its policy requiring written requests for refunds; the issuer was able to contact law enforcement before authorizing release of the funds.

Acquirers Use Fraud and Credit-Risk Policies and Controls That They Believe Address Money Laundering among Merchants

Most of the acquirers in our review told us that they did not have AML policies and programs targeted at the activities of merchants who agree to take their credit cards. Like issuers, however, the acquirers believed their fraud and credit risk policies and controls enabled them to help combat money laundering through credit cards, and yet they were also unable to cite instances of money laundering detected through their fraud controls.

[17]Regulation Z, 12 C.F.R. part 226, which implements the Federal Truth in Lending Act, 15 U.S.C. § 1601 *et seq* requires creditors to credit the amount of the credit balance to the consumer's account, refund the credit balance upon written request from the consumer, and make a good faith effort to refund to the consumer the balance remaining in the account for more than 6 months. 12 C.F.R. § 226.21 (2002).

As discussed earlier, Treasury believes that the systems the industry uses to monitor fraud alone are not sufficient and that the industry must consider additional factors and considerations specific to money laundering. The acquirers believed that through these policies and controls they were able to identify and reject most merchants who had engaged in or could potentially engage in fraud, including possible money laundering. Similarly to the issuers, the acquirers applied fraud and credit risk policies and controls to screen and monitor merchants for potential fraud or money laundering.

The acquirers told us that their screening process included:

- verifying the merchant's application against external sources of information such as the Better Business Bureau or Dunn and Bradstreet;
- performing some on-site visits to the merchant's facility to determine the legitimacy of the merchant's operations; and
- matching the merchant's name against industry negative lists.

Some acquirers further stated that their screening was also used to enforce prohibitions against accepting certain types of merchants, such as those engaged in gambling or selling pornography. Most of the acquirers said that they denied approval to merchants who were not creditworthy or were found on industry negative lists. A few of the acquirers acknowledged that questionable merchants who had no prior record of criminal activity and who had not appeared on industry negative lists could escape the scrutiny of their screening procedures.

The acquirers said that they monitored approved merchants, and they believed that their monitoring revealed most instances of possible fraud, money laundering, or other acts of misconduct that are capable of being detected; moreover, their monitoring enabled them to take timely and appropriate action against merchants, they said. To monitor the merchants, some acquirers told us that they initially developed a profile of the merchant, based on information from the screening process. The profile includes key information on the merchant, such as the merchant's type of business, expected credit sales, sales volume, average dollar amount of sale, and "chargebacks."[18] The profile might also involve classifying the merchant's business as low risk or high risk depending, for instance, on whether card transactions are conducted in the presence of the cardholder (such as in a restaurant) or not (such as in Internet sales). The acquirers explained that if a merchant's transactions were out of pattern, unusual, or suspicious, the acquirers' automated monitoring systems would flag these transactions, allowing the acquirers to take appropriate actions. All of the acquirers said that, if warranted, they would terminate relationships with merchants for fraud or misconduct. Some acquirers also said that they might freeze the merchant's account, file a SAR, and put the merchant's name on an industry negative list.

[18]A chargeback is a fee charged by a merchant service provider against a merchant account for a credit card transaction that had to be removed from a merchant's account. Chargebacks are permitted for several reasons, including, for example, disputes between the individual cardholder and the merchant that arise when the cardholder does not receive purchased services or goods, among others.

Major Card Processors Use Fraud-Focused Policies and Programs to Support Clients' AML Efforts

None of the three credit card processors we spoke with required their clients to have AML policies and programs, and all relied on U.S. banking regulators or host country regulators to ensure that their clients had AML policies and programs. One of the three processors said it did not perform due diligence on the financial institutions referred to it but, instead, relied on the credit card associations for this, particularly to perform due diligence on financial institutions from foreign countries. The other two processors said that they performed due diligence on their clients but focused on the operations and finances of the issuer-clients or on the credit and fraud management processes of the acquirer-clients. Nevertheless, one of these processors said that it conducted OFAC screening on all agent bank clients,[19] many of whom are located in foreign countries. Neither of the processors currently conducts business in any country that FATF has designated as an NCCT.

The three credit card processors we spoke with provided their issuer- and acquirer-clients with card processing and fraud detection and prevention services. Officials from these processors told us that even though they performed card processing functions for their clients, their clients retained responsibility for certain aspects of card processing, such as issuing cards, developing fraud and AML policies and programs, establishing the controls over card transactions, and making decisions concerning the results of card transactions, such as canceling accounts**.** The processors nevertheless believed that the range of services they provided contributed to their clients' efforts to identify cases of possible money laundering and enabled their clients to take appropriate action.

Some of the services that the processors identified as key among those they provided the issuer-clients included application processing, card activation, and fraud- and risk-scoring. In providing application processing services, officials of one of the processors stated that their company verified the applicant's identity and credit history by matching application information against external information sources, such as credit bureau records or public records, and industry negative lists known for fraud. Officials from this processor said that their company's application processing services provided the client-issuers with the means to accept or decline an

[19]An agent bank is a bank that is authorized by another third party (an individual, corporation, or bank), called the principal, to act on the latter's behalf. The agent bank may perform bankcard processing for a financial institution, including merchant card processing.

application based on known or potential problems with fraud or creditworthiness. Two of the processors told us that they performed card activation services; this requires verification of the cardholder's identity by phone or point of sale before the card is activated.

All three processors told us that they provided fraud- and risk-scoring services, which entail monitoring cardholder or merchant transactions. The processors said that these services involve developing or applying the scoring products to identify and report potentially fraudulent or financially risky cardholder behavior or activity. According to a processor, the clients rely on the reports and, as a result, are able to select strategies and take appropriate actions, such as conducting further investigation, declining authorization, or canceling accounts. Additionally, two of the processors—who provided services as acquirers or on behalf of acquirer-clients[20]—said that the acquiring services they provided their clients were focused on potential merchant fraud and credit losses. These processors said the services included significant due diligence and verification procedures in connection with the opening of merchant accounts. They also performed ongoing risk management or fraud monitoring of established merchant accounts.

Regulatory Oversight for Anti–Money Laundering Requirements Is Not Focused on Credit Card Operations

We found during our review of the credit card industry that issuing banks were the only entities in the industry that were subject to regulatory oversight for AML requirements. Bank regulators told us, however, that since credit cards were considered a low risk to money laundering, they limited the resources expended on overseeing bank credit card operations for adherence to AML requirements. We also found that while acquiring banks were subject to AML requirements, the regulatory oversight of these entities was focused on safety-and-soundness issues. The associations and third-party processors are currently subject to regulatory oversight solely covering their data processing systems and internal controls. The Patriot Act required the associations to establish AML programs by April 24, 2002. It is too early to tell how effective the Patriot Act requirements will be regarding the associations' AML programs.

[20]Processors who perform acquiring services secure merchants (like an acquiring bank) and bear a higher degree of liability than processors who merely assist in processing merchant transactions for an acquirer.

Regulatory Oversight of Issuing and Acquiring Banks' Credit Card Operations Is Focused Less on AML Requirements because of Lower Perceived Risk

The regulators we interviewed told us that although they examined issuing banks for adherence to the BSA and other AML requirements, they spent less of their examination resources on the credit card operations of these banks than on other operations. The regulators told us that during their AML reviews of issuing banks,[21] they must confirm, among other things, that the banks have the following in place:

- written BSA/AML policies and programs;
- senior management involvement in the process;
- mechanisms for suspicious activity reporting and large currency–transaction reporting;
- BSA/AML training programs for employees; and
- internal audit reviews of the BSA/AML policies and programs.

Some regulators told us that they also performed reviews more specific to credit cards. For example, they determined whether or not the bank could identify unusual transactions with respect to credit cards, such as prepayments. They also reviewed the account-opening and fraud-monitoring programs of these banks.

While regulators examined issuing banks for adherence to AML requirements, they expended less of their resources on the credit card operations of the bank than on other areas considered at higher risk to money laundering. Regulatory officials told us that, in their view, credit cards were considered a low risk to money laundering because the banks' application screening process, systems for monitoring fraud, and policies restricting cash payments and prepayments made credit cards less vulnerable to money laundering than other areas of the bank.

Consequently, regulators told us that most of their AML examination resources were dedicated to higher-risk areas of the bank, such as private banking, correspondent banking, or wire transfers.

[21]These are known as BSA examinations. These examinations are part of safety-and-soundness examinations for the Federal Reserve and the Federal Deposit Insurance Corporation, and part of consumer compliance examinations for the Office of the Comptroller of the Currency.

The regulators told us that while the acquiring banks were subject to the BSA and AML requirements, their examinations of these entities focused on safety and soundness because these entities were not viewed as being at high risk for money laundering. We found that two of the acquiring banks we met with had not been subject to any BSA/AML examination by the regulators. In one case, the acquirer was created as a Joint Venture in which a bank and a nonbank third party credit card processor each held 50 percent interests in the venture. The transaction processing services for the Joint Venture were performed by the non-bank third party credit card processor. Officials speaking on behalf of the Joint Venture noted that while the bank that held a 50 percent interest in the venture was subject to regulatory oversight (including oversight with respect to the BSA), it was less clear to what extent the Joint Venture itself (or the services provided by the nonbank third party credit card processor) was subject to the same oversight. The officials indicated that no regulatory examination of the Joint Venture had taken place. Nevertheless, these officials stated that the Joint Venture had decided to develop procedures to voluntarily file SARs. The other bank had a very small acquiring operation. Regulators told us that because the acquiring business accounted for only a small percentage of the overall business of the bank and because they applied a risked-based approach to their oversight of the bank, they did not examine this business. They did, however, review the examination of the acquiring business conducted by the bank's internal auditors.

Associations and Third-Party Processors Have Not Been Subject to AML-Related Requirements or Oversight

The associations and third-party processors[22] are currently subject to regulatory oversight by an interagency group of federal banking regulators under the auspices of the Federal Financial Institutions Examination Council.[23] The purpose of the oversight is to ensure that these entities pose little or no risk to the banks they service. The actual examination of these entities focuses on the integrity of the data processing systems and internal controls of the entity.

Associations Now Required to Have AML Programs

The Patriot Act required financial institutions, including operators of a credit card system or associations, to establish AML programs by April 24, 2002. The programs must include, at a minimum:

- the development of internal policies, procedures, and controls;
- a compliance officer;
- an ongoing employee training program; and
- an independent audit function to test the programs.

Under BSA regulations, the Internal Revenue Service is the regulatory body that will oversee the associations' adherence to the new requirements, unless Treasury delegates this authority to another agency.

[22]The third party processors are examined and regulated pursuant to the Bank Service Company Act (BSCA) 12 U.S.C. 1867 (c). The BSCA provides that "whenever a bank that is regularly examined by an appropriate federal banking agency, or any subsidiary or affiliate of such a bank that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises: (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the bank itself on its own premises, and (2) the bank shall notify such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first." 12 U.S.C. 1867(c).

[23]The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and to make recommendations to promote uniformity in the supervision of financial institutions.

As authorized by the Patriot Act, Treasury developed interim final rules prescribing minimum standards for the AML programs that associations are required to have in place pursuant to the Patriot Act. The interim final rules provide a definition for an operator of a credit card system, which includes associations, and provide guidance in complying with AML program requirements. The rules require, among other things, that by July 24, 2002, the associations

- develop and implement a written anti–money laundering program, approved by senior management, that is reasonably designed to prevent the operator of a credit card system from being used to facilitate money laundering and the financing of terrorist activities. At a minimum, the program must incorporate policies, procedures, and internal controls designed to ensure that:

  - the association does not authorize or maintain authorization for any person to serve as an issuing or acquiring institution without the associations taking steps based upon a risk assessment analysis to guard against the use of the credit card system for money laundering or for the financing of terrorist activities;

  - for purposes of making the risk assessment, the rule lists entities that are presumed to pose a heightened risk of money laundering or terrorist financing. An example is a foreign shell bank that is not a regulated affiliate.

- designate a compliance officer who will be responsible for ensuring that the AML program is implemented effectively and updated as necessary to reflect changes in risk factors, and that appropriate personnel are trained;

- provide for education and training of appropriate personnel concerning their responsibilities under the program; and

- provide for an independent audit to monitor and maintain an adequate program.

The requirement to assess money laundering and terrorist financing risks applies to both prospective and existing issuing or acquiring institutions. However, Treasury expects those institutions that pose a higher risk to money laundering to be reviewed by the associations with greater frequency.

The third-party processors who are not financial institutions are not covered directly under the Patriot Act, according to Treasury officials. However, these officials indicated that the processors would have obligations under the Patriot Act if they conduct banking functions for banking clients.

Agency Comments and Our Evaluation

We provided copies of a draft of this report to the Department of the Treasury and two of its bureaus, the Office of the Comptroller of the Currency and FinCEN; and to the Board of Governors of the Federal Reserve System and to the Federal Deposit Insurance Corporation. The agencies provided us with oral comments in which they generally concurred with the substance of the draft report. The Federal Reserve and Federal Deposit Insurance Corporation, however, noted that there was no evidence to suggest that credit cards were at a high risk for being used for money laundering. The Federal Reserve believed that it was correct in allocating its bank examination resources to other areas at higher risk for being used for money laundering, such as private banking and wire transfers. Treasury believes that the lack of detected instances of money laundering does not compel the conclusion that no money laundering risks exist. Treasury will continue to work with law enforcement, the regulators, and industry to identify both money laundering risks in the credit card industry and possible improvements that should be made in detection and prevention. The agencies also provided us with technical changes or factual updates, which we incorporated in this report as appropriate.

As agreed with your office, unless you publicly release its contents earlier, we plan no further distribution of this report until 30 days from its issuance date. At that time, we will send copies of this report to the Secretary of the Treasury, the Chairman of the Federal Reserve Board, the Comptroller of the Currency, and the Chairman of the Federal Deposit Insurance Corporation. Copies will also be made available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Key contributors to this report were José R. Peña, Elizabeth Olivarez, Sindy Udell, and Desiree Whipple. If you have any questions, please call me at (202) 512-5431 or Barbara I. Keller, Assistant Director, at (202) 512-9624.

Sincerely yours,

Davi M. D'Agostino, Director
Financial Markets and Community Investment

Scope and Methodology

To develop information on the vulnerabilities to money laundering in the credit card industry, we obtained views of and requested documentation from representatives of the credit card industry, bank regulatory officials, money laundering experts from the banking industry and academia, and law enforcement officials. We asked law enforcement officials from the U.S. Department of the Treasury (Treasury) and the U.S. Department of Justice for information about any cases they were aware of pertaining to credit cards and money laundering. At Treasury, we queried officials from the Internal Revenue Service, the U.S. Secret Service, and the U.S. Customs Service. At the Department of Justice, we queried officials from the U.S. Attorney's Office; however, they did not respond to our query. We requested that Treasury's Financial Crimes Enforcement Network (FinCEN) analyze the Suspicious Activity Report (SAR) database to determine the extent of SARs that pertained to credit cards and potential money laundering. We also reviewed news articles related to money laundering, and reviewed court summonses (provided by the Internal Revenue Service) related to the use of credit cards in offshore accounts. We requested documentation of existing AML programs—both broad AML programs and those specific to credit cards—from industry representatives. However, only three institutions provided this documentation. The others described their AML programs but were unwilling to provide documentation to support their descriptions because of concern about the confidentiality of proprietary policies. We also requested documentation from the credit card associations related to the reviews they conducted on offshore banks that were identified in a Senate Permanent Subcommittee on Investigations report on Correspondent Banking. We received documentation from one association. The other association did not provide any documentation, citing, among other things, confidentiality laws in these offshore jurisdictions as a reason for not providing us with the documentation. They also told us that they could not locate the paperwork with respect to the reviews they conducted on these offshore banks.

To obtain an understanding of industry efforts to address the potential vulnerability of credit cards to money laundering, we reviewed 20 major U.S. entities engaged in key aspects of the credit card process: 2 credit card associations, 9 credit card issuing banks, 6 acquiring banks, and 3 third-party processors. The criteria we used to select the entities for our review included responsibility for significant credit card activity in domestic and foreign markets and oversight by the various federal banking regulators. We conducted structured interviews of the entities we selected for our review. The 2 credit card associations we selected are the largest associations in the United States and internationally. The 9 credit card

issuing banks we selected ranked among the top 11 issuers in the United States and were responsible for about 74 percent of the outstanding receivables in the credit card industry. The acquiring banks we selected were affiliated with the issuing banks we reviewed. Of the 6 acquiring banks we selected for our review, 3 reportedly ranked among the top 10 acquirers in the United States. The 6 acquirers were responsible for 57 percent of the total sales volume of merchant transactions in the U.S. for 2001. In general, we selected credit card processors that provided services for the issuers in our review. Two of the 3 card processors we selected told us that they ranked as the 2 top U.S. card processors. These 2 card processors provided services to 5 of the issuers in our review. Finally, 2 of the 3 processors we reviewed provided services for issuers and acquirers in foreign countries.

To determine the existing regulatory mechanisms to oversee the credit card industry for adherence to anti–money laundering (AML) requirements, we interviewed officials from the Board of Governors of the Federal Reserve System (Federal Reserve Board), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC). We also conducted structured interviews of examiners from the OCC and the Federal Reserve System (Federal Reserve) who had responsibility for examining the issuing banks and some acquiring banks that we reviewed. We reviewed documentation of examination procedures for the Bank Secrecy Act (BSA) and related AML requirements, which we obtained from the Federal Reserve Board, FDIC, and OCC. We also reviewed documentation related to oversight of the associations and third-party processors, which we obtained from the Federal Reserve Board. We also discussed the new AML program requirements of the Patriot Act with Treasury officials, and the impact of the requirements with officials of the 2 associations.

We performed our work in Washington, D.C.; New York, New York; and San Francisco, California, between August 2001 and May 2002, in accordance with generally accepted government auditing standards.

Demographic Information about the Credit Card Issuers, Acquirers, and Processors in Our Review

To study the industry, we reviewed 9 credit card issuing banks, 6 credit card acquirers, and 3 third-party credit card processors. This appendix presents information about these entities for the year ending 2001.

Table 3 provides demographic information about the 9 credit card issuing banks that we selected for our review. As detailed in table 3, the 9 issuing banks were reported as being among the top 11 credit card issuers in the United States in terms of outstanding receivables and active credit card accounts. As of the year ending 2001, the combined total of accounts receivable of the 9 issuers (about $457.6 billion) represented about 74 percent of the total of accounts receivable throughout the industry ($622.5 billion), based on information from *The Nilson Report*.[24] The 9 issuers accounted for about 67 percent of active credit card accounts throughout the industry (181 million of an estimated 269.2 million cards). Seven of the issuers are engaged in diverse activities, offering products such as checking, savings, credit card or investment accounts. The other 2 issuers are monoline businesses, deriving their income primarily from credit cards. Six of the 9 issuers also provided acquiring services.

Table 3: Selected Characteristics of the Issuers in GAO's Review (Year Ending 2001)

Issuer	Type of business	Rank in order of outstanding receivables	Total outstanding receivables[a] ($ millions)	Number of active credit card accounts[a] (thousands)	Issues credit cards in foreign markets	Provides acquiring services
A[b]	Diverse Banking	1	$99,510	33,180	Yes	Yes
B	Monoline	2	74,909	20,278	Yes	No
C[b]	Diverse Banking	3	68,200	25,140	No	Yes
D	Diverse Banking	4	51,390	19,500	Yes	Yes
E[b]	Monoline	5	47,980	23,700	No	Yes
F	Diverse Banking	6	40,900	14,300	No	Yes
G	Diverse Banking	7	32,653	18,397	Yes	No
H	Diverse Banking	8	31,975	23,085	Yes	No
I[b]	Diverse banking	11	10,107	3,470	Yes	Yes
Total			**$457,624**	**181,050**	**6**	**6**

[a]Some figures provided in this table are estimates.

[24]*The Nilson Report*, Oxnard California, Issue 760, March 2002.

[b]The issuer maintains foreign correspondent banking relationships but does not market credit cards through these correspondent banks.

Sources: Figures used in this table are from *The Nilson Report*, Oxnard, California, Issues 756, 758, and 760, January, February, and March 2002, respectively, and GAO's analysis of responses received from the issuers.

Seven of the 9 issuers are members of the 2 major credit card associations and relied on the associations' networks to carry out their card transactions. In contrast, the other 2 issuers carried out their card transactions from automated networks they own and operate; each of these entities acts as both issuer and acquirer. Also, as shown in table 3, 6 of the issuers reported that they issued cards in foreign countries, but none of the 9 issuers markets cards in countries on the OFAC's list of sanctioned countries.

Table 4 presents information about the 6 acquirers selected for our review. The 6 acquirers also participated in our review as issuers, since 6 of the 9 issuers in our review were also engaged in acquiring services. Together, the 6 acquirers accounted for about 57 percent of the total industry wide purchase volume from credit cards ($652.4 billion out of $1.134 trillion) based on information from *The Nilson Report*.[25] The total number of merchant outlets in the United States is estimated to be about 4.9 million. Many of the outlets accept credit cards from more than one of the issuers in our study. Two of the 6 acquirers perform acquiring services in foreign markets.

Table 4: Selected Characteristics of Acquirers in GAO's Review (Year Ending 2001)

Acquirer	Number of outlets[a]	Purchase volume ($ billions)	Number of merchant clients
A	4.1 Million	$91.4	unknown
B	3.1 Million	224.5	unknown
C	490,000	114.3	390,000
D	224,869	42.3	165,362
E	201,577	175.8	67,675
F	4,652	4.1	3,950

[a]Figures for some of the outlets are estimates.

[25]*The Nilson Report*, Oxnard, California, Issue 760, March 2002.

Sources: Figures used in this table are from *The Nilson Report*, Oxnard, California, Issues 756, 758, and 760, January, February, and March 2002, respectively, and GAO's analysis of responses received from the acquirers.

Table 5 describes the services that the 3 major credit card processors in our review provided for the issuers and acquirers we reviewed. Of the 3 processors, 2 provided services for 5 of the issuers. The processors provided, at the issuers' direction, issuing, authorizing, and account billing services, among others. The processors also provided acquiring services such as verifying merchant account information, monitoring merchant transactions, or providing software products to monitor merchant transactions. Two processors were also engaged in acquiring merchants on their own behalf.

Table 5: Selected Characteristics of Credit Card Processors in GAO's Review (Year Ending 2001)

	Processor services			
Processor	**Issues cards**	**Authorizes transactions**	**Bills accounts**	**Provides acquiring services**
A	Yes	Yes	Yes	Yes
B	Yes	No	Yes	No
C	Yes	Yes	Yes	Yes
Total	**3**	**2**	**3**	**2**

Source: Analysis of responses to GAO review.

Organizational Structure of the Associations in Our Review

Each of the two associations in our review is owned by its member financial institutions that issue bankcards, or authorize merchants to accept those cards, or both. VISA International (VISA) is owned by about 21,000 member financial institutions and is a private, non-stock, for-profit Delaware membership organization composed of competing members, and is a corporation with limited liability. MasterCard International Incorporated (MasterCard) is a private, non-stock, Delaware membership corporation. Approximately 20,000 financial institutions participate in the MasterCard and related systems. MasterCard has two levels of membership; principals and affiliates. The principal members have a direct relationship with the association, while the affiliates are sponsored by principal members. For example, an offshore bank that has a correspondent banking relationship with a principal member can apply to become an affiliate if the principal sponsors the offshore bank. Principal members are responsible for their affiliates' behavior.

MasterCard recently changed its corporate status by creating a stock holding company, MasterCard Incorporated, which owns substantially all the voting power and all the economic rights in MasterCard. MasterCard Incorporated also recently acquired Europay International S.A., which has exclusive licensing rights in Europe for certain MasterCard brands. In connection with these transactions, each of MasterCard's principal members and Europay's shareholders received shares in MasterCard Incorporated and membership interests in MasterCard, which will continue to be the principal subsidiary of the holding company. MasterCard also acquired 100 percent interest in Mondex International, a global electronic cash company, on June 29, 2001.

Regional Structure of Associations

VISA is organized into six geographic regions—each with a Board of Directors—serving member financial institutions in the region. These regions are:

- VISA Asia Pacific;
- VISA Canada;
- VISA Central and Eastern Europe, Middle East, and Africa;
- VISA European Union;
- VISA Latin America and the Caribbean; and

- VISA U.S.A.

VISA U.S.A and VISA Canada are separately incorporated group members of VISA International. The other four regions are part of VISA International, which is incorporated in the United States.

MasterCard is organized into the following geographic regions:

- Asia Pacific;
- United States;
- South Asia/Middle East/Africa;
- Latin America/Caribbean; and
- Europe.

Functions of the Associations

The role of the associations in the day-to-day management of their operations is very similar, although each association is managed independently. Generally, each of the associations is responsible for the following activities with regard to members and merchants participating in their respective acceptance and payments systems:

- establishing standards and procedures for the acceptance and settlement of each of their members' transactions on a global basis;
- providing a global communications network or providing technical standards supporting communications over public communications networks, for interchange; that is, the electronic transfer of information and funds among members;
- conducting the due diligence for the financial soundness of potential members and requiring periodic reporting of members on fraud, chargeback, counterfeit card, and other matters that may impact the integrity of the association as a whole;
- developing marketing programs that build greater awareness of the brand;
- conducting customer service with member institutions;

- enhancing and supporting the marketing activities and operational functions of the members in connection with the association's programs and services; and

- operating the security and risk systems to minimize risk to the member banks, including operating fraud controls to allow members to monitor transactions with their cardholders and establishing specific design features of the bankcard to enhance security features.

Officials from one of the associations indicated that their association is now conducting due diligence for money laundering risks presented by existing and potential members.

Association Funding of Operations

The associations rely on a mix of revenue sources to support themselves, largely based on brand and transaction fees generated when a bankcard is used. To a lesser extent the associations support themselves with varied membership fees, registration fees, and other fees, such as user fees, which are fees charged to members for services they elect to receive from the association. For example, one association charges members for fraud monitoring services. Officials from one of the associations indicated that their fees are structured to give members an incentive to issue cards and increase purchase sales volume.

Board of Directors

VISA International's Board of Directors is made up of representatives from each of the regional boards, and it governs the association's global policies and rules. Each region has its own Board of Directors, which governs policies and rules within that region. The Board of Directors for the U.S. region has two classes of directors, one appointed and the other elected. Those member institutions that have a certain percentage of the association's overall sales volume may appoint board members. The other directors are elected by member vote, based upon a slate of candidates recommended by the association's management. VISA International's Board of Directors is elected in the same manner as the U.S. region's Board of Directors. Since VISA does not issue stock, it calibrates the number of votes to its members by providing those with greater sales volumes, a greater number of votes on the Board of Directors. The President and Chief Executive Officer of the U.S. region is also on the U.S. Board of Directors. The Chairman of the Board of the U.S. region is elected by the directors and is from a member bank.

VISA International's Board of Directors is responsible for setting policies and procedures, appointing officers, approving the budget, and so forth. The regional boards pass by-laws and regulations related to operations for their particular region. For example, in some regions of the world, short-term interest cannot be charged, so the regional board would accommodate its rules for these cases. The Boards of Directors for the regions can pass any rule, as long as it is not inconsistent with the global policies and rules.

MasterCard has a Board of Directors that is made up of officials from member financial institutions in addition to the MasterCard Chief Executive Officer. This Board of Directors has responsibility for the following:

- deciding on the compensation of the association's Chief Executive Officer;
- deciding whether to license, deny, or drop members from the association;
- authorizing major decisions; and
- developing and updating the by-laws.

MasterCard Board members are elected by principal members of MasterCard.

Licensing of Banks in Offshore Jurisdictions

Officials of one of the associations told us that in order to license a bank located in the United States or in an offshore jurisdiction to become a member, the bank first had to submit a detailed application to the association. The regional Board reviewed the application to assess the ability of the bank to provide the benefits of the association's service to cardholders, and required a majority approval to allow the bank to become a member. The association officials provided us with an application for membership only in the U.S. region, but stated that the application for the international regions was similar. The application required information from the applicant to demonstrate its ability to meet membership obligations, based on financial capacity and ability to manage projections for the program it has arranged with the association. The application is vetted by the local region relative to local and global standards, and includes the following:

- the name and legal address of the principal;
- the name of the signing officer;
- the name and address of the sponsor, and whether the bank had any affiliation with a nonfinancial institution;
- the name and contact information for fraud and investigations;
- the applicant's financial information (for example, the balance sheet, income statement, and so forth); and
- the potential earnings or sales volume over a period of three years.

Officials from the other association told us that in order to license an offshore bank to become a member, the bank first had to submit a detailed application to the association that was reviewed, among other things, to ensure that the bank met the association's eligibility requirements. We were not provided with a copy of the application, and thus are unaware of what type of information the association requested from the applicant. The regional Board of Directors reviewed the application, and the Board required a majority approval to allow an offshore bank to become a member. The association also conducted a risk assessment on the potential member to determine if the member presented undue financial, legal, or other risks to the association. In addition, once a member was accepted into the association, the association's security and risk departments would conduct monitoring of the member for activities such as fraud, chargebacks, and counterfeit cards to identify issues before they developed into significant problems for the association. If problems were identified, the security and risk departments would investigate and, if necessary, perform audits or reviews of relevant member banks to determine whether sanctions or corrective actions were required.

Officials from both of the associations indicated that the due diligence procedures for membership from international or offshore banks was very similar to that for U.S. member banks. As described earlier in this report, these procedures included:

- obtaining documentation showing that the bank is licensed and subject to bank supervision and regulation in the jurisdiction where it is licensed;

- applying underwriting procedures to ensure that the bank is financially sound and can meet its financial obligations; and

- obtaining assurances that the bank will abide by the association's rules and regulations and comply with applicable laws of the bank's home country.

Officials of one of the associations told us that in addition to relying upon the laws and regulations of an applicant's home supervisory authority, each of the association's regions had its own underwriting standards that were tailored to the unique characteristics of the region or country. Each region might require additional steps for underwriting and membership, but this was up to the region and might be based on differences unique to each region. Generally, the association officials indicated that the association did not conduct in-depth due diligence on the signing officer on the application, and did not get the names of the Board of Directors of the applicant institution or the names of other principals. These officials indicated, however, that they have obtained this information in isolated circumstances. The association officials indicated that the association's regions assume a minimum level of due diligence by the government agency that had chartered the institution, and the association relied on this government agency to obtain information on the signing officers, Board of Directors, and principals of the institution.

The officials of this association also indicated that lacking a legal framework to do so prior to the implementation of the Patriot Act, the association did not have a policy to identify banks that may be using its payment system for potential money laundering activities. However, the officials indicated that the association has implemented programs in compliance with the Patriot Act requirements since its enactment. If one of the member banks were engaging in this activity using the association's payment system, the association now believes there is sufficient information, including information collected through formal procedures and informal networks, in addition to requests from law enforcement and government authorities, to highlight potential activity of this nature in the system. If the association learned that one of its member banks was owned or controlled by criminals such as drug traffickers, the association would review the facts, consult with legal authorities, and if necessary and appropriate, take steps to terminate its relationship. The association has taken steps in this regard in the past.

Officials from this association also indicated that the legal framework prior to the enactment of the Patriot Act did not provide the association with categories of countries, or help the association determine which countries have what are now considered to be lax money laundering regulations. These officials indicated that U.S. member banks are not allowed by U.S. laws and regulations to issue cards that can be used in Office of Foreign Assets Control (OFAC) countries. However, member banks in other countries can issue cards that can be used in OFAC countries. For example, a French member bank can issue bankcards to a non-U.S. citizen that can be used at a merchant in Cuba, but no U.S. issuer would authorize or settle this transaction.

Officials from the other association stated that prior to the passage of the Patriot Act, the association followed the same standards for U.S. and offshore banks in allowing them to become member institutions. That is, all financial institutions seeking membership in the association, whether located in the United States or elsewhere, were reviewed to determine whether they met the association's eligibility criteria. Officials from this association indicated that their review was intended to ensure that financial institutions presenting unreasonable financial, legal, or other risks were not admitted into its system, although the reviews did not specifically focus on money laundering issues. As we mentioned earlier in this report, this association indicated that as a result of its implementation of an anti–money laundering (AML) program required by the Patriot Act and approved by senior management, it will now look closely at its licensing documents and other information to review its members for money laundering risks. This association will review its entire membership in the United States and abroad. It will review such things as potential members' backgrounds before doing business with them, to ensure that the association will not be a system abused by money launderers. The association will first focus on those jurisdictions with lax AML laws and other jurisdictions deemed to involve high risks of money laundering–related activities. The risk management, security risk, and licensing groups will play key roles in the new AML program.

Observations on Money Laundering Scenarios

We presented the issuers, acquirers, and examiners in our review with six money laundering scenarios and invited comments about the most appropriate due diligence procedures for avoiding possible money laundering in each case. We also asked for descriptions of any limitations that might be encountered in carrying out such procedures. The issuers, acquirers, and examiners commented selectively on the scenarios, choosing not to comment on some scenarios. None of the scenarios reflected the policies, procedures, or practices of any of the participants in GAO's review. The scenarios and the comments we received are summarized below. The examiners' comments do not represent the official position of the federal banking agencies.

Scenario 1

In this hypothetical scenario, money launderers establish a legitimate business in the U.S. as a "front" for their illicit activity. They establish a bank account with a U.S.-based bank and obtain credit cards and ATM cards under the name of the "front business." Funds from their illicit activities are deposited into the bank account in the United States. While in another country, where their U.S.-based bank has affiliates, they make withdrawals from their U.S. bank account, using credit cards and ATM cards. Money is deposited by one of their cohorts in the U.S. and is transferred to pay off the credit card loan or even prepay the credit card. The bank's on-line services make it possible to transfer funds between checking and credit card accounts.

Comments on Scenario 1

The two acquirers and two issuers who commented on this scenario agreed that conducting due diligence on the merchant at the opening of the account would be key in preventing this merchant from obtaining an account. The issuer stated that the burden of such due diligence belonged to the acquiring bank that established the merchant's deposit-taking account. Moreover, the issuer said that due diligence should include an on-site inspection and analysis of the merchant's cash flow. In discussing due diligence that would be adequate, the two acquirers emphasized their own procedures, which reportedly included a thorough verification of the merchant or principal owners, screening of the merchant against a fraud database or the OFAC list of individuals, and, for a private banking unit, the application of "know your customer" rules. One acquirer also referred to its automated monitoring system, which would reportedly track merchant transactions by size and rate and flag overseas transactions. This acquirer described limitations in carrying out due diligence procedures by noting

that without a reason to suspect a merchant, the acquirer would have no reason to suspect that merchant's money was "bad money."

The examiners for six of the issuing banks concurred that the bank that opened the account for the business should conduct appropriate due diligence to determine the legitimacy of the business. Some indicated, for example, that the bank should visit the business and should understand the nature of the business and type of activity expected of the business, including the size, frequency, and types of payments that are most typical of the business. Some examiners expected the bank to monitor the business for deposit activity, including monitoring for potential structuring. One also expected the bank to monitor the account for significant changes, such as prepayments going to credit cards. Another examiner stated that despite the due diligence conducted on a business, including site visits, an illegitimate business could still appear legitimate. The examiner stated that continued monitoring of the business was therefore important.

Scenario 2

This scenario is not hypothetical, but involves a closed bank in the Cayman Islands. The bank's president admitted to using its correspondent banking relationship with a U.S.-based credit card processor to obtain credit cards on behalf of its clients, some of whom were money launderers. These clients used credit cards to facilitate access to illicit funds held in the offshore bank.

Comments on Scenario 2

One issuer who also provided acquiring services said that large issuers have sophisticated fraud detection systems. However, the issuer indicated that it would be difficult for a bank such as the one presented in this scenario to detect fraud and, thus, potential money laundering if the funds deposited by the clients engaged in money laundering appeared to be legitimate. The issuer also said that money launderers conducting cash transactions through the major credit cards would risk detection as a result of the authorization and identification procedures.

Three of the six examiners indicated that the U.S.-based credit card processor should have performed due diligence on the bank in the Cayman Islands. Two of the examiners stated that the U.S.-based banks that had correspondent relationships with the Cayman Island bank should also have conducted due diligence, including reviewing the AML policies and procedures of the Cayman Islands bank. According to the examiners, review of the AML policies and procedures is important since the U.S. bank

has no knowledge of the customers of its correspondent bank. One examiner stated that regulators were suspicious of correspondent relationships in jurisdictions with lax AML controls, and further noted that the Patriot Act requires U.S. banks to obtain more information on foreign correspondent accounts of banks located in such jurisdictions.

One examiner said that although the credit card processor should have performed due diligence on the Cayman Islands bank, money laundering would have been difficult to detect. Another examiner stated that a bank president's complicity in a money laundering scheme would make that money laundering next to impossible to detect.

Scenario 3

In this hypothetical scenario, the bank is located in a foreign country with lax anti–money laundering (AML) regulations. The foreign bank is owned by drug dealers and accepts their illicit funds. The bank becomes an issuing bank as a result of its existing correspondent relationship with a U.S. bank. Consequently, the drug dealers are also able to get credit cards from this bank and use them to obtain cash advances of their illicit funds or make purchases within the U.S. and other countries. They also make credit card payments to the foreign bank using illicit funds.

Comments on Scenario 3

The one issuer commenting on this scenario stated that the rules for obtaining cash advances through credit cards, which are standard throughout the world, work against money laundering. For instance, a U.S. bank must perform identification matches and authorizations of new transactions, thereby revealing the identities of potential money launderers. The issuer also said that the credit card associations are expected to conduct an investigation of the issuing bank before giving permission to the bank to issue credit cards.

Three of the six examiners who responded to this scenario indicated that under the Patriot Act, U.S. banks are required to obtain documentation of the ownership of foreign banks. Five of the six examiners indicated that the U.S. bank needed to conduct additional due diligence on the correspondent bank, given that it is located in a jurisdiction at high risk for money laundering. Some of the additional due diligence would include:

- understanding the bank's ownership and structure;
- knowing how the bank is regulated;

- assessing the bank's management, additional financial statements, licenses, and certificates of incorporation; and
- reviewing business references and identification.

Scenario 4

In this hypothetical scenario, money launderers submit false documents to obtain a merchant account with a U.S. bank and often use their credit cards to cover the start-up costs of establishing their "front business." The money launderers also create false information and submit false identification and other information to the bank to establish their "merchant account." They commit bank fraud to establish a false merchant account and also conceal the original source of their income. Given this scenario, the merchant (or acquiring) bank accepts the credit sales draft and receives its commission from the transaction.

Comments on Scenario 4

Only one issuer, also engaged in acquiring services, offered substantive comments on this scenario. This bank stated that to identify the activities of the merchant in this scenario, the acquirer would have to verify that the merchant was physically located at the address given to the bank, perform a background check on the merchant, and develop a profile of the merchant's transactions that would be used for monitoring the merchant. Two acquirers commented that the same controls discussed in scenario 1 applied in this scenario.

The examiners also said that the acquiring bank needed to conduct due diligence up front to determine the legitimacy of the business and monitor the account for unusual transactions. The examiners' description of the due diligence included site visits of the business, verifying the business through third parties such as Dunn and Bradstreet, and obtaining credit bureau reports and financial statements. The examiners also expected the acquiring bank to compare actual transactions with expected transactions, with major differences triggering an investigation of the merchant.

Scenario 5

In this hypothetical scenario, a criminal is able to open up a number of credit card accounts with different issuers. The criminal prepays each of the cards with a few thousand dollars and then leaves the country with the prepaid cards. He does not report that he has prepaid credit cards worth

more than $10,000 when he leaves the country. Once overseas, he is able to withdraw cash or purchase items with the credit cards.

Comments on Scenario 5

Four issuers offered comments on this scenario. Three stated that there would be no way for a bank to know if a cardholder maintained credit balances on multiple credit cards from different issuers. One issuer commented that under this scenario, a bank must ensure that it has controls covering prepayments of credit card accounts or controls that monitor prepayments creating a credit balance. The four issuers stated that they monitored credit balances, and credit balances triggered their systems. They also stated that they applied additional controls over credit balances. For example, they imposed limits on cash withdrawals. These limits varied among the issuers. For example, one issuer mentioned that if the customer had a $10,000 credit balance and $5000 cash withdrawal line, amounting to a $15,000 credit balance, the bank would allow the customer to access only $5,000, thereby preventing the customer from accessing the total credit balance in a foreign country. Two issuers said that they would or have canceled customers with large credit balances, and one of these has also taken action to block related transactions. If the customer wanted a refund of the credit balance, all the issuers agreed that they would not automatically send a refund check. First, they said, that they would review the payment or perform some investigation. Two issuers additionally said that they would impose controls over a customer's attempts to access a credit balance while overseas. One said its systems would flag this, and his institution would file a SAR. The other said that her institution would impose limits over cash withdrawals made in a foreign country.

Five examiners responded to this scenario and three concluded, as did the issuers, that it was not possible for an issuing bank to know that its cardholder was carrying a credit balance with other issuers. Three examiners also indicated that the banks needed to have systems in place to monitor prepayments and credit balances.

Scenario 6

This scenario is similar to Scenario 5, except that the criminal ties together his checking and credit cards. The criminal places "dirty money" in a U.S. bank and establishes a checking and credit card account. He also obtains an ATM card. The individual then prepays his credit card account by about $8,000, by transferring funds from his checking account to his credit card account through the bank's ATM machine, or through on-line banking in the United States, or both. When the bank's system flags the prepayment, the

individual tells the bank that he is planning to go abroad and wants to ensure that he has sufficient credit for his purchases. Nevertheless, he prepays his credit card account several times more and gives the same reason for the prepayments to the bank. When the individual goes abroad, he goes to the bank's affiliate in a country known for lax AML laws and withdraws at least $3,000 in cash. He also makes a number of credit purchases from merchants who do not have electronic registers.

Comments on Scenario 6

An issuer offering comments on this scenario said that it subjects an individual to separate due diligence procedures for opening a checking account versus a credit card account. Further, the issuer said that the customer would also be subject to limitations on cash withdrawals. For example, if the customer used an ATM machine of another bank, the customer would be subject to the issuer's limits on cash withdrawals as well as the limits imposed by the other bank's ATM machine. The issuer stated that because a bank does not know if its customers are criminals, a credit balance alone does not appear to be criminal or suspicious. According to the issuer, sometimes customers use credit balances for travel and will call the bank proactively to inform the bank that they are paying an excessive amount on their credit card account for the purpose of travel.

One of the four examiners who responded to this scenario indicated that the bank should first monitor the deposit account to identify any suspicious activity. Three of the examiners indicated that the banks have systems to monitor prepayments, and that these types of prepayments would be flagged. One examiner stated that realistically, most banks would not allow prepayments like those specified in this scenario. Another examiner indicated that if a customer were truly in need of money while overseas, the bank should offer methods of obtaining it other than prepayments. This examiner indicated that if the customer were to repeatedly prepay the credit card, the bank should determine if these transactions are reasonable. If the transactions are not, the bank should close the account or take some other appropriate action.

Review of SAR Database on Potential Money Laundering through Credit Cards

As part of our effort to determine the vulnerability of the credit card industry to money laundering, we asked the Financial Crimes Enforcement Network (FinCEN) to review its suspicious activity report (SAR) database. FinCEN did not provide us with access to the SAR database or to the SARs the agency identified as the result of its review. We therefore relied on FinCEN to use our criteria, as described below, in reviewing the SAR database and to provide us with a report of the results.

We specifically requested that FinCEN review the SAR database for the 2-year period of October 1, 1999, through September 30, 2001, to identify and quantify reports with the following characteristics:

- Bank Secrecy Act/structuring/money laundering violations checked by the financial institution on the SAR form and the term "credit cards" specified in the narrative section of the form;
- Bank Secrecy Act/structuring/money laundering violations checked by the financial institution on the SAR form and the terms "debit card" or "ATM card" specified in the narrative section of the form;
- credit card fraud violations checked by the financial institution on the SAR form and the terms "Bank Secrecy Act," "structuring," or "money laundering" specified in the narrative section of the form;
- debit card fraud violations checked by the financial institution on the SAR form and the terms "Bank Secrecy Act," "structuring," or "money laundering" specified in the narrative section of the form.

FinCEN reported that its initial query of the SAR database using our criteria resulted in the retrieval of 669 SARs. FinCEN transferred these SARs to an excel spreadsheet to analyze the statistical portion of the report and also transferred them to a Word document for analysis of the narrative content. A FinCEN official indicated that each SAR was read and sorted according to methodologies as described by the filing institution. He indicated that duplicates were eliminated, as were SARs that had nothing to do with money laundering. For example, FinCEN eliminated reports that involved credit cards used as a form of identification, or statements by banks that the suspect had a credit card from a specific bank or had applied for a credit card. After the process of elimination, 499 SARs were identified as accurately responding to the criteria we stated above. These SARs represent about one-tenth of 1 percent of the SARs filed by financial institutions during the 2-year period we specified.

Most SARs Related to BSA/Structuring/Money Laundering Violations

FinCEN provided the following breakdown on the 499 SARs that were identified in the review:

- Financial institutions filed 488 (97.7 percent) of the SARs for BSA/structuring/money laundering violations;
- Eight SARs that were filed by financial institutions cited credit card fraud as the primary violation;
- Two SARs that were filed by financial institutions cited debit card fraud as the primary violation;
- One SAR that was filed by a financial institution cited defalcation/embezzlement as the primary violation.

FinCEN found that 134 financial institutions, including 1 foreign bank licensed to conduct business in the United States, filed the 499 SARs. The amount of money involved in the violations ranged from $0 to $9.76 million. Seven of the SARs filed by these institutions were for amounts in excess of $1 million. Seventy of the 499 SARs (14 percent) were referred directly to law enforcement by the financial institution, in addition to being filed with FinCEN. Of these, 39 were reported to federal agencies and 31 to state or local authorities.

Most SARs Were Isolated Cases

FinCEN found only a few cases in which 2 or more SARs were filed on the same individual or business. This indicated that activity reported on most of the SARs was considered "an isolated incidence" by the reporting banks, according to FinCEN. One exception involved 6 SARs that were filed in early 2001 on four suspects, which revealed that check payments credited to these individuals' credit card accounts were made by a fifth individual. This activity indicates that the subjects had ties to the person making the payments, according to FinCEN. This individual had been indicted on charges of money laundering, contraband cigarette smuggling, and visa/immigration fraud charges. This was the only incidence within the 499 SARs where a group of individuals could be linked to one another.

Cash Structuring Fairly Common in SARs Filed

FinCEN found that 115 of the 499 SARs (or 23 percent) described cash structuring activity in the narratives. Typically, the SARs described customers attempting to make multiple deposits in amounts under $10,000,

thus avoiding the Currency Transaction Report (CTR) filing requirement. Most often, the customers were attempting to deposit cash into various accounts, pay down loans, purchase cashiers' checks, and make credit card payments. When the customers were notified that a CTR would be filed based on the total amount of money transacted, most withdrew one or more transactions to get under the CTR threshold. This activity was routinely reported as suspicious by the financial institution. FinCEN noted that of particular interest was the high dollar amount customers wanted to pay on their credit cards. The attempted total payments were typically well over $5,000 and often exceeded $10,000.

15 SARs Reported Credit Card Overpayment, Which FinCEN Flagged as Adaptable to Money Laundering

FinCEN found that 15 of the 499 SARs (3 percent) were filed for overpayments on credit cards. The overpayments required the financial institutions to issue refund checks. According to FinCEN, overpayments and refund checks can be a means to launder money through credit cards, particularly if the funds used to overpay the card were derived from illicit activities. The refund check provides the means to convert the illicit funds into a legitimate bank instrument that can be used without question as to the origin of funds.

Of the 15 SARs, 7 discussed such payments being made in cash. Other methods to overpay the credit card involved checks written to the credit card account, electronic transfers between accounts, and payment via debit cards. The financial institutions were unable to determine the source of funds for 4 of these overpayments.

Suspicious Cash Advances Found in a Fair Number of Cases

FinCEN found that 97 of the 499 SARs (19 percent) were filed for suspicious cash advances. Typically, the customer used the advances to purchase cashiers' checks or to wire funds to a foreign destination. Some customers also requested that cash advances be deposited into savings or checking accounts. Most of the cash advances were structured to avoid the filing of a CTR.

ATM/Debit Cards Used in Structuring Schemes

FinCEN found that 70 of the 499 SARs (14 percent) discussed the use of ATM/debit cards. The individuals used these cards to structure multiple deposits or withdrawals to avoid triggering the filing of a CTR. Some of the SARs described customers who wired money into accounts from a foreign country, then made multiple ATM withdrawals in that foreign country.

Convenience Checks Used for Structuring

FinCEN found that 32 of the 499 SARs (6 percent) were filed for use of courtesy/convenience checks supplied by credit card issuers. Some of the checks were deposited into accounts in structured amounts. FinCEN noted that the use of these checks to structure deposits may warrant future scrutiny.

Wire Transfers Did Not Show Discernable Trend

FinCEN found that 16 of the 499 SARs (3 percent) were filed for wire transfer activity. FinCEN noted that there was no discernable trend or pattern in the case of wire transfers via the credit card industry. Some scenarios they found were the following:

- cash deposits followed by immediate wire transfers to credit card companies;
- incoming wire transfers from foreign countries to an individual's credit card account;
- outgoing wire transfers to credit card accounts;
- incoming wire transfers followed by checks written to credit card companies; and
- cash advances used to wire funds to foreign destinations.

Three SARs filed by a single financial institution described incoming wire transfers from a foreign location payable to a credit card corporation. The aggregate total of the amounts transferred by wire, as reported in these SARs, was $11,824,982.90.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00