citigroup

Michael A. Ross
General Counsel
Global Consumer Business

Citigroup Inc.
399 Park Avenue
New York, NY 10043

Tel 212 559 9788
Fax 212 793 0072
michael.ross@citicorp.com

November 28, 2000

Robert H. Hast
Managing Director
U.S. General Accounting Office
Office of Special Investigations
441 G Street N.W., Room 6K17S
Washington, D.C. 20548

Dear Mr. Hast:

In connection with a request by the Permanent Subcommittee on Investigations of the Senate Governmental Affairs Committee, you identified a series of bank accounts opened or referred to one of our Citibank branches by a Russian businessman, Irakly Kaveladze, since 1991. Citibank senior management became aware of these accounts in July 2000, when they were brought to our attention as a result of your inquiry and the subpoena for information related to the accounts that the Subcommittee issued at your request. We promptly retained outside counsel to review this matter.

We have detected no illegal activity in the Kaveladze-related accounts, all of which are now closed. However, the number of accounts he opened or referred and the volume and type of activity in these accounts were not adequately understood at the time, even though Citibank's policies met or exceeded industry standards throughout the period that Mr. Kaveladze was a customer and referral source. It is clear in hindsight that our systems and tracking procedures were not sufficient to detect the nature and extent of his relationship with us. Given enhancements to our systems and procedures, we are confident that we would detect questionable activity and take action more promptly should a similar situation arise today.

For example:

- At the time of greatest activity in the Kaveladze-related accounts, the Branch and Compliance did not have systems to monitor wire transfers for questionable activity. Today, Compliance monitors all incoming and outgoing wire transfers in business and consumer accounts that aggregate over predetermined thresholds in a single month.

- At the time, the Branch undertook only limited due diligence on businesses referred by Mr. Kaveladze, instead relying on Mr. Kaveladze, a customer, to attest to their legitimacy. Today, account opening requirements for businesses require more thorough due diligence.

- At the time, Compliance lacked the systems necessary to detect the number of accounts that one individual had opened or referred. Today, the systems are in place so that as soon as questionable activity is identified in one account, Compliance reviews all accounts opened by the same signers. We are developing, and will soon implement, additional enhancements that will track within the branch network multiple accounts referred by a single individual or using the same address.

- At the time, these Branch employees showed little sensitivity to the need to review or monitor account activity or question the number of accounts opened for one address. Today, compliance training has been significantly strengthened, sensitivities are heightened, and our commitment is enforced with audits and accountability.

- At the time, the Branch failed to close accounts promptly when Compliance determined they should have been closed. Today, processes are in place to ensure there is appropriate tracking and follow-up when compliance determines an account should be closed.

A list of the issues raised by this episode, and the improvements we have instituted to address these issues, is presented in the attachment that follows.

In an effort to assist your inquiry, we offer the following specific information we have learned about the accounts associated with Mr. Kaveladze.

Mr. Kaveladze Opened 28 Accounts Since 1991

Mr. Kaveladze opened his first account in October of 1991. He identified himself to the Branch as an export/import broker and provider of incorporation services that assisted Russian nationals in incorporating in the U.S. and establishing U.S. bank accounts. His business was called International Business Creations (IBC).

Prior to opening Mr. Kaveladze's first account, the Branch Manager and Sales Manager at the Branch personally met with him and inquired about his background and business. Mr. Kaveladze impressed them as a professional, college-educated Russian businessman who spoke fluent English and was seeking to aid other Russians in securing a stable environment in which to invest and save the proceeds of their business activity at a time when Russia was experiencing political and economic upheaval. Mr. Kaveladze presented the documentation then required by the U.S. consumer-based branch business at Citibank ("Citibanking"), before opening any accounts, including two forms of identification for his consumer account and articles of

incorporation for his IBC account that showed IBC was incorporated in Delaware. Over the next few years, Mr. Kaveladze opened another 27 accounts on which he was a signatory.

Mr. Kaveladze also obtained a credit facility for IBC, which was fully secured and initially set at $900,000 in 1992. In the course of the credit approval process, Citibanking representatives met with Mr. Kaveladze several times, spoke to IBC's accountant, undertook a UCC search, and reviewed Mr. Kaveladze's passport and personal financial statement, as well as IBC's incorporation documentation. IBC was reviewed annually thereafter, which involved personal visits to Mr. Kaveladze's office, a Dun & Bradstreet check, a UCC search, and a review of Mr. Kaveladze's personal financial statement, audit information and tax returns. Mr. Kaveladze's line of credit was increased to $2 million in 1993 and maintained until 1995, when he apparently obtained more favorable terms from another bank. Each IBC letter of credit was supported by airway bills, invoices, bills of lading and packing slips that verified shipments of shoes from various places throughout the world (Italy, Spain, New York, Brazil and France) to Moscow.

Mr. Kaveladze Referred 108 Accounts Since1991

Shortly after opening his first account, Mr. Kaveladze began referring other Russian individuals and businesses to Citibank. From January 1992 to January 2000, Mr. Kaveladze referred at least 108 individuals and businesses to Citibank (sixteen of these accounts were never active), all but seven to the specific Branch where he commenced his relationship with Citibank. Each of these accounts used IBC's address as its account address.

Before opening a business account for a business customer referred by Mr. Kaveladze, the Branch appears to have followed procedures and required a completed and signed application form; two executed signature cards for each signer; two forms of identification, including one with a photograph, for each signer; and a CHEX inquiry to verify social security number validity for each signer where applicable. The Branch also required an Employer Identification Number (EIN); a copy of incorporation documents and a certified tax identification number.

Before opening a consumer account for a customer referred by Mr. Kaveladze, the Branch appears to have followed procedures and required two forms of identification including one with a photograph; a CHEX inquiry to verify social security number validity where applicable; a completed and signed application form, and two executed signature cards. Two of the individual account holders (who were also employees of IBC) had overdraft protection on their checking accounts, which Citibanking considers an extension of credit; one of them also had a revolving line of credit using real property as collateral. None of the other Kaveladze-related account holders sought or was extended credit by Citibanking.

Today, Citibanking's account opening requirements for businesses such as the Kaveladze-referred businesses are significantly more stringent. The Kaveladze-referred businesses were incorporated in the United States and had a U.S. address, but had foreign signatories and were physically located outside of the United States. Today, foreign signatories must also have a bank or employment reference mailed directly to Citibanking. In addition to the above requirements, today, Citibanking requires offshore corporations and import/export companies to provide evidence of their business activity by furnishing two or more copies of two of the following: invoices, shipping documents or contracts.

Today, Citibanking also requires an out-of-state corporation to provide, in addition to all of the documentation and verifications described above, a certificate of authority to do business in the state and county where the account is being opened. Foreign businesses must provide foreign incorporation documents with a written English translation and a letter of authenticity from the U.S. consulate or apostille from the country of origin in addition to a bank reference.

Additionally, Citibanking is now developing, and will shortly implement, a procedure for branch personnel to record in account opening documentation the name of the individual or business that referred the new account. This information will be used so that all accounts referred by one individual can be easily identified.

At The Time, Account Opening Procedures Did Not Require The Signatory To Be Present

At the time most of these accounts were opened, Citibanking's policies did not require account signers to be present to open an account. Initially, the Branch permitted customers referred by Mr. Kaveladze to open accounts without the account signer making a personal visit, as long as the Branch obtained the required documentation and the account signer personally visited the Branch shortly thereafter. It appears that at least some of these accounts remained open, even when the account signer failed to appear. However, because Citibanking did not issue checks or an ATM card before a personal visit, the only activity that should have occurred in these accounts was deposits. For this reason, the accounts that were opened without the presence of the signer typically had no activity. In approximately 1995, the Branch closed all of the inactive accounts and began requiring that the signers on all accounts referred by Mr. Kaveladze be present before an account could be opened.

In 1998, Citibanking formally established a policy requiring all branches to meet personally with account signers before any small business and professional accounts can be opened.

Activity in the Accounts Opened by Mr. Kaveladze Reached Nearly $275 Million Over a Nine Year Period.

As much as $275 million passed through accounts opened by Mr. Kaveladze from the time he opened his first account in 1991 to the present (around $400 million, if transfers between Mr. Kaveladze's own accounts are included). Another $450 million passed through accounts he referred during this period, for a total of $725 million in all accounts (or $850 million if transfers between Mr. Kaveladze's accounts are included). Most of the total activity in the accounts that Mr. Kaveladze opened or referred was concentrated in 11 accounts ($600 million of the $725 million, or nearly 85%), four of which were Mr. Kaveladze's own accounts. The bulk of all account activity (approximately $617M or 72.7%, which includes transfers between Mr. Kaveladze's accounts) occurred prior to May 1996, before SAR reporting requirements went into effect, before Citibanking developed the capacity to monitor wire transfers, and before Russia was first designated by the State Department as high risk for money laundering.

At all times during which Mr. Kaveladze had a relationship with Citibanking, the Branch with which he had the relationship had a total of approximately 1800 business accounts. The number of open Kaveladze-related business accounts in any given year, by contrast, did not exceed 66, less than 4% of the Branch's business accounts. (A chart summarizing the number of Kaveladze-related accounts in any given year is attached.) In the aggregate, the average monthly balances for all of the Branch's business accounts totaled in the $20-23 million range. In the aggregate, the average monthly balance for the Kaveladze-related business accounts was $1 million, but did reach a high of $3 million during one month in 1995. Because of the nature of the account activity, the Kaveladze-related accounts were not particularly profitable; over eight years, it appears Citibanking made less than $300,000 in total from all these accounts combined.

All of the accounts referred or opened by Mr. Kaveladze are now closed.

The Branch's Ability to Review Account Activity Was Limited

Although meeting or exceeding industry standards prevailing at the time, in hindsight, Citibanking had limited means to monitor the activity in the accounts opened or referred by Mr. Kaveladze, prior to mid-1996. Citibanking branches systematically monitored cash deposits, but few of the transactions in the Kaveladze-related accounts were cash. Most of the activity was conducted through wire transfers and, as is the common practice in the banking industry, most of the wire transfer activity in the accounts was done directly by the customer without having to make direct contact with the branch. Accordingly, branch employees typically did not have knowledge of wire transfer activity in these accounts.

Today, Compliance monitors all incoming and outgoing wire transfers over predetermined thresholds in any given Citibanking business or consumer account. Compliance reviews every Citibanking account in which these transfers occur in geographic areas identified as high-risk by the U.S. Government (e.g., Cyprus, Russia, Colombia), or where the transfers reflect activity unusual for the

customer or business. For any account where the wire transfer activity exceeds the monitoring threshold but is not investigated, Compliance is required to document reasons for not pursuing further investigation.

At the time, the only tool available to the Branch for systematic monitoring of account activity was the daily Balance Fluctuation Report (BFR), which reported changes in the balances in each account at the end of each day from the preceding day. These reports were available only to the Branch Manager and the Branch's Operations Manager and were used primarily for fraud and loss control and as a marketing tool for flagging large deposits that might suggest a customer would be receptive to a sales call about investment opportunities. Although the Branch could use the BFR to question any unusually large transactions, from a compliance perspective it was an imperfect tool (reflecting only the net change for a given day and not individual credits and debits) and the Branch appears to have used it for this purpose only rarely.

On the one documented occasion when the Branch did detect from a BFR a transaction in a Kaveladze-related account that it regarded as suspicious, the Branch Manager made appropriate inquiries. In July 1994, the Branch Manager noted a $1,000,000 wire transfer into the IBC account and a wire transfer out of the account in the amount of $850,000 three days later. The Branch Manager called Mr. Kaveladze for an explanation of this activity and was told that the funds were earmarked for a business deal in Brazil and, as it turned out, the receiving party could accept only a $150,000 disbursement. As a result, the party in Russia that originated the transfer requested that the balance be returned. Subsequently, the Branch Manager sought advice from Citibank's Loss Control division about this activity. A Loss Control representative reviewed the transaction and informed the Branch Manager, apparently without elaboration, that it was not a concern. We have been unable to determine the basis for this reassurance as the Loss Control representative is deceased and his files were not maintained.

Today, Citibanking branch employees are instructed on how to use the BFRs as compliance tools. Today, the branch manager is required to report questionable transactions to Compliance, which, unlike in 1994, has the expanded capacity to investigate suspicious activity. In addition, the branch manager is today designated as an Anti-Money Laundering Coordinator and held responsible for failing to report any unusual activity to Compliance.

Citibanking provides anti-money laundering training for all of its new branch employees. In addition, each branch holds quarterly compliance meetings, at which anti-money laundering regulations and issues are presented and discussed. Once each year at these meetings, branch personnel view an anti-money laundering videotape. This videotape is replaced periodically; the latest version includes segments from the November 1999 Senate hearings on money laundering. Compliance also issues periodic bulletins to the branches with updates on anti-money laundering issues. In response to developing sensitivity as to what characteristics suggest a high risk of money laundering and increased

sophistication in anti-money laundering detection techniques in the regulatory and financial communities, Citibanking has dramatically enhanced its anti-money laundering training over the period since Mr. Kaveladze opened his first account.

At The Time, Compliance Resources Were Not Adequate by Today's Standards

The capacity of Citibanking's Compliance unit to monitor account activity has expanded substantially from the time Mr. Kaveladze opened his first account, in keeping with the development of various anti-money laundering statutes and regulations. From only one employee in 1991 and no automated monitoring, today, the compliance operation supporting our U.S. branch banking system employs 16 people and uses automated and increasingly sophisticated monitoring techniques. Until April 1996, Citibanking's Compliance unit monitored only cash transactions and could not monitor wire transfers. Nor was there a way to identify accounts that were referred by the same customer or that had the same address. Compliance did not have effective tools for monitoring wire transfer activity and could not track the activity of potentially related accounts that did not bear the same account name.

Thus, Citibanking's Compliance unit did not become aware of IBC until 1995, when it learned that Mr. Kaveladze had requested that Citibank provide a speaker for a conference he was sponsoring ("Offshore Strategies '95") for the stated purpose of helping East European and Russian businessmen integrate into the world financial community. Although Citibank declined the speaker request, Compliance learned that the Branch Manager already had provided a letter to Mr. Kaveladze welcoming conference participants and offering to help them with their international banking needs. This conference, together with the Branch Manager's endorsement, prompted Compliance to undertake a closer look at the IBC accounts.

This Know Your Customer (KYC) review included a review of IBC account activity, invoices, bills of lading, and a customer contact memorandum reflecting a 1994 visit to IBC. Compliance also verified that IBC's primary client, Crocus International, was a legitimate shoe distributor in Russia that formerly employed Mr. Kaveladze. Compliance, concluding that the Know Your Customer supported Mr. Kaveladze's characterization of IBC as a business consulting service and shoe merchant, found no problems with the IBC accounts.

Although the Branch understood that Mr. Kaveladze's relationship with Citibanking went beyond his IBC accounts -- the files related to all of the accounts opened or referred by Mr. Kaveladze were kept together -- Branch personnel were not required to, and did not, explain to Compliance that Mr. Kaveladze was a signer on other accounts, in addition to the IBC accounts, or that he had referred dozens of other customers who all used the IBC address. Thus, Compliance completed the Know Your Customer review on IBC without appreciating the significance of Mr. Kaveladze's relationship to the Branch.

Citibanking is developing, and will soon implement, the ability, when investigating a particular account, to identify and examine all other accounts

using the same address as or that were referred by the same person who referred the account under investigation. These measures, which are being implemented prospectively, will ensure that a Know Your Customer review of an account like IBC would detect all other accounts opened or referred by someone like Mr. Kaveladze. Furthermore, branch managers are now required to determine the extent of Citibanking's relationships with business customers and report to Compliance all relationships characterized by prescribed criteria.

Mr. Kaveladze's relationship with Citibanking came to the attention of Compliance again in the spring of 1996 when it learned that from 1993-1995, Mr. Kaveladze had assisted nearly 50 Russian non-resident aliens in obtaining secured Citibank credit cards, each cardholder using IBC's address. Citibank South Dakota's Card Products department ("Cards") had identified these accounts the preceding year to determine whether the card holders were a front for IBC. At that time, Cards had contacted the Branch and learned that IBC had been a bank customer since 1992 and that its business was to assist Russians in conducting business in the United States by providing incorporation services and facilitating banking relationships. Facilitating the obtaining of credit cards and, in some instances, providing the security required for card holders without a credit history, was consistent with this business.

The Branch's description of IBC reassured Cards, so the cards were not canceled at that time. Over a period of several months, however, Cards and Compliance continued to consider the situation and ultimately, the decision was made to close the card accounts.

Thereafter, Compliance determined that it would also direct the Branch to close the IBC accounts. The Branch resisted this direction. There was inadequate follow-up and the IBC accounts were not closed until March and April 2000.

In addition to acquiring the capacity to identify all account holders with the same address, Citibanking has instituted a process that ensures there is appropriate tracking and follow-up when Compliance determines an account should be closed. This function is aided greatly by organizational enhancements to the compliance program. The compliance function in all businesses now has a stronger reporting relationship to the Office of General Counsel and uses the results of our audit capability to correct deficiencies. Further, Citigroup's new Director of Global Compliance coordinates and oversees compliance across all Citigroup businesses.

After Citibanking's Compliance unit began monitoring wire transfer activity in April 1996, it detected a number of wire transfers involving Kaveladze-related accounts that fit the characteristics of possibly suspicious activity: transfers from or to offshore banks in high-risk jurisdictions other than the account holder's own country. Many of these transfers did not name the beneficiaries. In some instances the Branch obtained documentation and explanations from Mr. Kaveladze concerning these transactions. However, Compliance still found the transactions suspicious, made appropriate

regulatory filings, and directed the branch to close 11 of the accounts as a result of activity detected from wire transfer monitoring.

Since then, all of the accounts referred or opened by Mr. Kaveladze have been closed.

Processes and Systems in Place Today Would Detect Kaveladze-like Activity

We have detected no illegal activity in the Kaveladze-related accounts. Nonetheless, Citibank is concerned that this relationship developed without Citibanking fully comprehending the Branch's relationship with Mr. Kaveladze and without a complete review of each business customer and the account activity it generated. Throughout the period of greatest activity in these accounts (1992-1995), Citibanking's capacity to monitor account activity and its understanding of the kinds of account activity that should generate questions was, in hindsight, not sufficient to detect the breadth and implications of this customer relationship, even though it conformed with prevailing industry practices. Although subsequent enhancements to Citibanking's account monitoring capacity did begin to flag some activity in these accounts, only recently did Compliance learn the full extent of this relationship and the scope of the account activity.

Measured against today's standards, Citibanking's handling of these accounts falls short of the diligence and attentiveness now required. However, given the state of knowledge about risks associated with the type of activity occurring in the Kaveladze-related accounts at the time this activity was actually occurring, and Citibanking's limited ability to monitor wire transfer activity at the time, we cannot fairly measure conduct then against today's standards. To date, we have not detected evidence of deliberate violations of requirements in place at the time. However, much time has elapsed since many of these events occurred and many employees involved have retired, died, or found employment at other companies.

Citibank has always complied with the anti-money laundering standards set by regulators. It was only in 1996 that the U.S. Government designated Russia as a high money laundering risk. Early money laundering regulations and regulatory guidance focused on cash transactions rather than on wire transfers; therefore, Citibanking's training and systems also focused on cash transactions. Furthermore, the U.S. Government did not issue the current regulations requiring suspicious activity reporting or wire transfer record keeping until 1996.

As soon as these regulations were enacted, Citibanking promptly responded. We began to train employees with regard to suspicious wire activity. Further, as awareness of money laundering activities by the regulators and the banking community increased, Citibanking increased its anti-money laundering training activities, requiring employees to view anti-money laundering videos and attend quarterly compliance meetings, and sending frequent bulletins educating employees concerning compliance issues.

Today, each Citibanking branch is audited annually for its compliance with anti-money laundering and Know Your Customer policies, and managers are held accountable for the results.

Since learning of its vulnerability to development of account relationships without full appreciation of their scope or characteristics, Citibanking has undertaken a review of its entire base of business customers to identify any other circumstances in which multiple customers are using the same address. This review is ongoing.

Today, there are processes and monitoring in place at Citibanking, summarized in the attached grid, that ensure closer scrutiny at the time such relationships are established and detect questionable account activity at the time it occurs. Specifically, systems are already in place or under development and will soon be in place to:

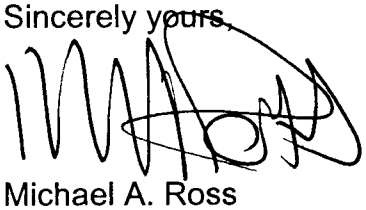
- ***Ensure that when employees open a new account, the name of the reference is recorded so Compliance can in the future systematically identify all accounts referred by the same individual.***
- ***Ensure that in the future all business accounts on which the same individual is a signer or reference can be routinely identified, if the number of such accounts exceeds a specified number.***
- ***Ensure that whenever a specified number of accounts have the same address, the accounts are routinely flagged.***
- ***Ensure that all large incoming and outgoing wire transfers above certain thresholds are monitored.***
- ***Ensure that stringent account opening requirements for foreign businesses and foreign nationals are properly met.***
- ***Ensure that Branch Managers are held accountable for determining the extent of Citibanking's relationship with a particular business customer and reporting all relationships to Compliance that are characterized by prescribed criteria.***
- ***Ensure appropriate follow-up on accounts Compliance determines should be closed.***

Given the dramatic enhancements we have made to our compliance policies, programs, processes, technology and staffing, we are confident we would detect such questionable activity today and take prompt and appropriate action. Procedures are or shortly will be in place to detect the opening of numerous accounts listing the same address or referred by the same person, to identify questionable wire transactions and patterns of activities, and to assure certain and swift action by both the branch and by our Compliance Unit.

The heightened sensitivity to the risk of money laundering, both within Citigroup, as a result of our extensive training programs and policies, and in the global financial community in general, also assures that we are more vigilant in establishing ways of detecting and preventing money laundering as perpetrators become more sophisticated. As we have said in the past, Citibank is committed to being at the forefront of anti-money laundering efforts, and continues to institute enhancements to its programs and capabilities to prevent abuse.

Please let us know if we can be of further assistance.

Sincerely yours,



Michael A. Ross

Cc: Hon. Susan Collins
Hon. Carl Levin

We have detected no illegal activity in the Kaveladze-related accounts, all of which are now closed. However, the number of accounts he opened or referred and the volume and type of activity in these accounts were not adequately understood at the time, even though Citibank's policies met or exceeded industry standards throughout the period that Mr. Kaveladze was a customer and referral source. It is clear in hindsight that our systems and tracking procedures were not sufficient to detect the nature and extent of his relationship with us. These systems and procedures have since been strengthened. Given these enhancements, we are confident that we would detect questionable activity and take action more promptly should a similar situation arise today.

ISSUES	RESOLUTIONS
• At the time, the Branch and Compliance did not have systems to monitor wire transfers for questionable activity.	• Today, systems are in place to systematically monitor all outgoing and incoming wire transfer activity above predetermined thresholds daily and monthly.
• At the time, the Branch undertook only limited due diligence and instead relied on a customer to attest to the legitimacy of referred businesses.	• Today, account opening requirements for businesses require more thorough due diligence, including: 1. site visits; 2. evidence of business activity (at least 2 invoices, shipping documents or contracts); 3. evidence of authority to do business (certifications from state and county authorities); 4. foreign incorporation documents with a written translation in English and a letter of authenticity from the US consulate or apostille from the country of origin; 5. a bank reference for the business; 6. a bank or employment reference and identification for each signer;
• At the time, Compliance lacked the systems necessary to detect the number of accounts that one individual had opened or referred.	• Today, the systems are in place so that as soon as suspicious activity is identified in one account, Compliance reviews all accounts with the same signer. • We are developing, and will soon implement, additional enhancements that will enable Compliance to track within the branch network multiple accounts referred by a single individual or using the same address.
• At the time, these Branch employees showed little sensitivity to the need to review or monitor account activity or question the number of accounts opened for one address.	• Today, compliance training programs have been significantly strengthened, sensitivities are heightened and our commitment is enforced with audits and accountability.
• At the time, the Branch failed to close accounts when Compliance determined they should have been closed.	• Today, processes are in place to ensure there is appropriate tracking and follow-up when Compliance determines an account should be closed.

IK-RELATED ACCOUNTS BY YEAR

YEAR	BUSINESS ACCOUNTS OPENED	CONSUMER ACCOUNTS OPENED	BUSINESS ACCOUNTS CLOSED	CONSUMER ACCOUNTS CLOSED	TOTAL IK-RELATED OPEN ACCOUNTS	AVERAGE MONTHLY BALANCES IN TOP 11 ACCOUNTS*
1991		2			2	**
1992	5	3			10	**
1993	18	5			33	$166,957
1994	36	4	2		71	$844,426
1995	15	2	21		67	$2,194,217
1996	13	3	9		74	$772,390
1997	11	2	6		81	$906,693
1998	12		6		87	$556,555
1999	2	1	13	1	76	$140,145
2000	1		56	21	0	$45,091

* The activity in these 11 accounts constitutes nearly 85% of the activity in all 136 of the IK-related accounts.
** Data unavailable.