September 15, 2003

PLAINTIFF'S EXHIBIT 231

Keith Duckett
Vice President - Director
Internal Audit Division
175 Water Street – 14th Floor
New York, N.Y. 10038
Voice: (212) 458-3300
Fax: (212) 458-3255

To: M.R. Greenberg

RE: *Internal Audit Report #03-164*
Auto Warranty Run – Off Operations

Our audit of the auto warranty run–off operations revealed that overall controls are satisfactory and that the run-off process has been managed effectively and efficiently. We've made recommendations to further improve controls as the business continues to run-off. Paid losses have decreased from $90M in 2001 to $58M for year ended 12/31/02; and are currently at $18M for the six months ended 6/30/03. Claims should continue to decrease until 2007 when all warranties will have expired. Management agrees with most of our recommendations and has taken corrective action; responses are included in the body of the report. In some instances management will evaluate the feasibility of implementing our recommendation given that the business is in run-off. The more significant control issues are summarized below.

We noted differences in paid loss amounts reported and amounts booked in LMS; a total of $9.6M had not been booked as of April 2003. Controls over cash receipts should be strengthened to ensure that incoming checks are properly accounted for and safeguarded and that there is adequate segregation of duties. Payments received for contract transfer fees are not recorded, as a general ledger account for this bank account was never established. Additionally, there is no reconciliation of contract transfers processed to fees received. We noted a backlog in processing data received from TPAs; management has made the reduction of the backlog a priority. Physical access to the LAN room should be further restricted, logical access controls should be enhanced to comply with corporate standards and security administration procedures should be documented. Application administrators for the claims system should ensure that user IDs are individually assigned and passwords are periodically changed.

Conclusion: Based on our evaluation of the internal control structure, the degree of compliance with existing controls, and results of auditing procedures, we have assigned a rating of "2" - satisfactory compliance, to the Auto Warranty Run – Off operations.

Keith L. Duckett

70 Pine St.
M. Castelli (3/70)
L. English (18/70)
M. Maloney (34/70)
K. Murray (21/70)
R. Rifkin (54/70)
B. Rothenberg (38/70)
R. Sandler (21/70)
H. Smith (18/70)
M. Stark (54/70)
M. Sullivan (18/70)
E. Tse (17/70)
G. Williams (7/70)
J. Yu (3/70)

175 Water St.
R. Beier (17/175)
P. Brucato (14/175)
P. Calbi (14/175)
P. Carruba (14/175)
N. Faulkner (30/175)
R. Jacobson (30/175)
E. Kohl (14/175)
K. Moor (30/175)
J. Scampas (30/175)
C. Schader (30/175)
T. Tizzio (30/175)

90 Hudson St., Jersey City
F. Lungo (8/90)
M. Popolano (6/90)
R. Messing (8/90)
T. Sebben (8/90)
M. Wein (9/90)

80 Pine St.
M. Paffmann (5/80)

AMERICAN INTERNATIONAL GROUP, INC.
INTERNAL AUDIT REPORT
AUTO WARRANTY RUN-OFF

BACKGROUND AND SCOPE

The Internal Audit Division (IAD) has completed an audit of the Auto Warranty Run-Off operation. The purpose and scope of our audit was to review the adequacy of existing controls over the Auto Warranty claims operations, premium and claims processing, cash receipts and disbursements, financial reporting and general operations in the Maitland and Denver offices.

Our Information Systems Audit Group reviewed system interface and data balancing controls over data received from TPAs and downloaded into the AIG WARP database and the A/EGIS Claims system. A review was also performed of application security controls in the A/EGIS system. In addition, the IS Audit Group assessed the adequacy of controls in the LAN environment that supports Auto Warranty operations in Maitland, Florida. This included a review of physical security, data security, Windows NT Operating system security, data backup, environmental controls, and business and disaster recovery planning.

Our review was performed utilizing IAD computer based audit exception and flag reports that highlight potential variances from AIG standards and identify transactions that have a higher potential for exceptions. These reports were run for the period 1/1/02 through 4/30/03 and included multiple claims on contracts, claims per vendor, claims paid outside contract period, claims authorized over authority limit, claims paid over authority limit, claims paid on cancelled policies, and duplicate payments.

This report is restricted to weaknesses noted and recommendations for improvement. It is not intended as a commentary on the favorable aspects of the Auto Warranty Run-Off operations.

Financials:

Paid Losses 2001	Paid Losses 2002	Paid Losses YTD 6/31/03
$90,224,334	$57,811,149	$18,022,276

I. PAID LOSS REPORTING

Controls surrounding the monthly coding of paid losses to LMS for the auto warranty business need strengthening. Each month the Denver office submits coding sheets of paid losses from the A/EGIS system to Claims Administration in Parsippany, NJ for coding into LMS, which ultimately feeds Corporate Record. IAD reviewed the losses reported in AEGIS to the booking in LMS from May 2002 through April 2003 and noted a net total of $9.6M has not been booked. Warranty and Claims Administration management are currently researching the differences.

RECOMMENDATION

Warranty management should perform monthly reconciliations of paid loss coding to LMS to ensure proper reporting. Any discrepancies should be researched and resolved with Parsippany Claims Administration management.

MANAGEMENT ACTION

After discussing the above recommendation with Claims Administration, it was agreed that:

- *Claims Administration has developed a tracking system to assist in monitoring the progress and completion of all requests received from Denver.*
- *The unit manager will be required to provide a weekly management status report of all outstanding items.*
- *Going forward, the unit manager will work directly with the Denver office, assisting them with the monthly reconciliation effort to research and correct any discrepancies.*

II. CASH RECEIPTS

Controls surrounding the cash receipts process in the Maitland and Denver offices needs strengthening. During our review IAD noted the following:

A. Safeguarding

Checks received in the Maitland office are not logged in the mailroom and restrictively endorsed immediately upon receipt. Checks that are received as payment for contract transfers are separated from all other cash receipts and delivered to the contract maintenance lead. The contract maintenance lead will log the transfer payments into a cash receipts log, which is located on a shared drive, but does not restrictively endorse the checks. These checks are then sent back to the mailroom to be mailed to the Denver office for processing. Prior to IAD's review, contract transfer fees were sent back to the Maitland office for deposit rather than going directly to the bank. All other receipts are delivered to the human resource assistant where they should be logged and restrictively endorsed. However, during IAD's review it was noted that two checks totaling $4k were not logged or restrictively endorsed.

RECOMMENDATION

All checks should be logged into a mailroom log and restrictively endorsed immediately upon receipt. This individual should sign the mailroom log indicating all checks have been received, and log them into a separate cash receipt log. A monthly reconciliation should be performed from the mailroom log to the cash receipt processing log to ensure all accountability of checks received. In addition, all cash receipts logs should be maintained on a secured drive with update capabilities limited to the one individual and their backup in charge of cash receipts.

MANAGEMENT ACTION

- *Management has instituted a mailroom check log and checks are now restrictively endorsed immediately upon receipt.*
- *All checks are delivered to the Administrative Assistant responsible for safeguarding all checks in the safe until proper disposition. The Administrative Assistant signs a mailroom log transmittal form to indicate she has received the checks from the mailroom. All checks received are then placed in the safe and entered into the checks in safe log. Only copies of checks are distributed to other employees, as needed.*
- *Contract transfer fees for confirmed transfers are now sent directly to the bank for deposit.*
- *In addition to auditing the checks in the safe to the log, AIWS is instituting an additional reconciliation between the mailroom check log and the checks in safe log.*
- *Change access to both the mailroom check log and checks in safe log are limited to the individuals responsible for maintaining the log and their back-up.*

B. System Access/Segregation of duties

Improvement is needed to ensure segregation of duties exist in access to the A/EGIS system. The individuals in charge of transfer payment cash receipts in the Maitland and Denver offices have update access in the contract fields of A/EGIS. In the Denver office, the individual responsible for cash receipts also processes contract transfers in the system.

RECOMMENDATION

Individuals that handle cash receipts should not have the ability to update contract information in the system.

MANAGEMENT ACTION

Management has restructured the job functions in Denver and Maitland to ensure the individuals handling the checks do not have update access in the contract fields in A/EGIS.

C. Contract Transfer Fees

- Payments received for contract transfer fees are not recorded. The contract information is changed to reflect the new contract holder, however, there is no system indicator that identifies a transfer has taken place and that the fee has been received. In addition, there is no reconciliation of processed contract transfers to the fees received.

- Deposits of contract transfer fees are made into a non-interest bearing checking account in Maitland along with cash received for recoveries of overpayments or legal settlements. This account was established in 1999 and has never been swept into a DBG pool account. The account itself was opened with an incorrect name (AIG Warranty Services of Florida instead of NHIC) and a GL for the account was never established. As of 3/31/03 there was $270k in the account.

RECOMMENDATION

Transfer fees should be recorded. Auto Warranty Run-Off management should investigate the feasibility of creating a contract transfer indicator field in A/EGIS where the fee received can be posted. This would allow for a proper reconciliation to be performed between contract transfers processed and fees received each month. This would also ensure that contracts are not transferred more than once as per contract terms. In addition, Auto Warranty Management should ensure a GL account is established for the revenue received for contract transfers as well as for the bank account used for recoveries and transfer payment receipts. Receipts should be recorded and bank reconciliations should be performed. This account should be periodically swept into a DBG pool account.

MANAGEMENT ACTION

- *ISG will prepare a time and cost estimate for the creation of a contract transfer indicator field in A/EGIS where fees received can be posted. After the cost estimate is received, management will weigh the costs and benefits of performing the additional programming, taking into account the short period remaining in the runoff period. If programming a contract transfer indicator field in A/EGIS is too costly, management will consider manual alternatives for reconciling contract transfers processed to the fees received.*
- *A general ledger account has been set up and a cash receipt has been submitted to properly recognize the revenue received to date. Cash receipts will be prepared for each new deposit. As part of the monthly bank reconciliation process the bank balance will be agreed the general ledger.*
- *Warranty management is in the process of establishing procedures with AIG Corporate Treasury to do an initial sweep of the account and to set up a schedule to periodically sweep the account into a DBG pool account.*

III. CLAIM PAYMENT PROCESSING

Controls need to be strengthened in the Maitland payment processing unit to ensure payment authority levels are adhered to. Currently, payment processor authority limits established in A/EGIS are higher than the authority levels per their credit card. Therefore, a payment processor could either process a check or close a payment out above their credit card limit. In addition, the claims adjusting manager has payment authority in the A/EGIS system of $10k as well as a credit card in his name with a single limit up to $15k.

RECOMMENDATION

Payment processors should have one established payment authority limit. These limits should be reflected in their A/EGIS system capabilities. In addition, since there is a separate payment unit, the claims adjusters should not have payment authority in the system or through credit cards.

MANAGEMENT ACTION

- *ISG will prepare a time and cost estimate to develop a payment authority level in A/EGIS, which will compare a payment specialist's payment authority to the amount of the payment to be issued. Currently the system looks at the total value of the claim, which artificially restricts the payment specialist's ability to make payments since a single claim frequently results in payments to multiple parties (e.g. repair facility, parts supplier, contract holder, rental car company, etc.).*
- *The Claims Manager's payment authority in A/EGIS has been revoked and his credit card has been cancelled.*

IV. VOIDED CHECKS

Controls surrounding voided checks needs to be strengthened. Currently, the Maitland office receives notification to void a returned CDCS check from the Denver office. The Denver office processes the void in the A/EGIS system while Maitland stamps the check void and cuts out the signature. The voided checks are maintained in Maitland. There is no reconciliation by Denver to ensure that all voids processed were properly defaced, and all checks defaced were properly voided in the system. In addition, the checks are not sent to draft administration in Parsippany for destruction.

RECOMMENDATION

The Denver office should require copies of the voided checks be sent to them in order to ensure all voids are properly processed. In addition, the voided checks should be sent to draft administration in Parsippany for destruction.

MANAGEMENT ACTION

The Denver office now requires copies of the voided checks to be faxed to them to ensure all checks voided in AEGIS are properly defaced. As an alternative to mailing the defaced checks to Parsippany, AIWS proposes shredding the checks in Maitland.

V. PROCESSING OF TPA DATA

ISG receives Auto Warranty cancellation data monthly from six TPAs. In addition, one TPA (ISI) submits paid loss information for a 100% cession to Lyndon for policies effective 2/1/99 and subsequent (Note there is no exposure to AIG on this cession). This data must be processed by ISG and loaded into AIG's WARP system as well as into Auto Warranty's A/EGIS claims system for statistical purposes. A review of this process revealed that ISG is four months behind schedule in loading this data into WARP. In April 2003, data in WARP was only current through October 2002, leaving November, December, January and February data waiting to be loaded. As of July 15, 2003, TPA data in WARP was current through January 2003, with February, March, April and May awaiting processing.

Failure to keep Auto Warranty contract information up to date leads to inaccurate financial reporting, and may result in paid losses on cancelled contracts. From 1/1/00 through 10/31/02, AIG paid approximately $202K on cancelled policies.

RECOMMENDATION

ISG should attempt to try to bring the processing of Auto Warranty data from the TPAs data up to date.

MANAGEMENT RESPONSE

Since upgrading our systems to SQL 2000 in June 2003, monthly and quarterly processing times have improved significantly. Bringing our data up to date is one of our high priority tasks at this time and we expect to be current by the end of September 2003.

VI. LAN CONTROLS

A. Physical LAN Room Review

During a tour of the LAN room containing the Primary Domain Controller (PDC), Backup Domain Controller (BDC) and various servers, backups and UPS devices, the following issues was noted:

- A water-stained ceiling indicated that there was a leak. The LAN room is located on the top floor and, per management; the roof leaked about three times (twice this year) during a routine cleaning of the roof.
- Cardboard boxes and plastic wrapper debris were found in the room.
- The first floor conference room, although locked, contains a switch and router rack accessible by various managers with keys.

Persistent water leakage may damage the IT hardware. The switch and router rack that share space in the first floor conference room allow unauthorized access to the equipment.

RECOMMENDATION

The environmental controls in the LAN room need to be strengthened. Network hardware should be protected from inadvertent and/or unauthorized access. Management should repair the leak, and speed up the installment of a drip pan to detect leaks. Additionally, the feasibility of partitioning a room for the switch and router rack with locked doors should be determined.

MANAGEMENT ACTION

- *Bids are being sought for a monitored drip pan and the building maintenance division has assured AIWS that leaks have been repaired. Several rainstorms over the past 30 days have resulted in no apparent leakage.*
- *All debris has been removed from the LAN room.*
- *Access to the first floor conference room is now limited to the General Manager, IT/Facilities/Special Projects manager and the LAN Administrator.*

B. LAN Room Access

A review of cardholders with access to the LAN room disclosed that 8 out of the 16 cardholders did not belong to the Information System department. An excessive number of cardholders with access to the LAN room create an unnecessary risk exposure.

RECOMMENDATION

Management should restrict access to the data center room to employees with appropriate job responsibilities.

MANAGEMENT ACTION

- *Access to the LAN room and the LAN Administrator's office is now limited to 5 individual's cards: The LAN Administrator, Manager, General Manager, City Fire Box, and the LAN Administrator's back-up.*
- *Since the audit was performed, the operation has been downsized from a staff of 106 to 61. In so doing, AIWS relinquished its lease to the third floor suite. The third floor suite formerly housed the PBX and phone system router, switch, and server and had to be consolidated into the LAN room on the fourth floor. It is necessary for our internal phone facilitator to have access to this equipment to update and maintain the phone system. Thus, there will be six individuals with access to the LAN room.*

C. Security Administration for LAN and A/EGIS

A review of the security administration procedures for NT LAN and the A/EGIS system revealed that there were no formal documented procedures for updating, deleting and creating new users. Without sufficient documentation, smooth transition may not be achieved during job rotation or reassignment and the efficient processing of system administration requests may be impeded.

RECOMMENDATION

A/EGIS and LAN security administration procedures should be documented.

MANAGEMENT ACTION

The preparation of a formal document outlining the procedures for updating, deleting, and creating new users for the NT LAN and A/EGIS systems has commenced.

D. LAN Audit Logs

Audit logging is set to monitor successful logon attempts, successful file access attempts and successful use of user rights. These NT LAN audit log settings are excessive. Auditing successful logon attempts, file access attempts, and use of user rights clutters up the audit log with unnecessary data and makes it more difficult for LAN administration to identify security violations.

RECOMMENDATION

Management should remove audit logging on successful logon attempts, file access attempts, and use of user rights.

MANAGEMENT ACTION

Audit logging of files access attempts and use of user rights has been discontinued. However, we intend to continue the audit logging of successful logon attempts for security purposes and business reasons. In the past, corporate IT or ISG personnel with LAN access have made changes to our servers, which resulted in discontinuation of certain necessary business applications. The audit logs have proven to be the best way to determine who made the changes in order to quickly solve the system outages.

E. LAN NT Built-in Groups

A review of the LAN NT built-in group account revealed the Account Operators group contained a User-ID that belonged to the assistant claims manager. Members in the Account Operators group can administer domain users and groups as well as create, delete and manage users, local groups and global groups.

RECOMMENDATION

The account operator user group should be restricted to appropriate LAN administrators. Management should remove the inappropriate user and limit access to account operators to authorized LAN administrators.

MANAGEMENT ACTION

The assistant claims manager no longer has access to the account operator group.

F. LAN ID Review

During a review of the NT LAN, a number of active User-IDs were discovered belonging to terminated users. Retaining unused LAN accounts increases the opportunities for unauthorized access.

RECOMMENDATION

The LAN administrator should periodically perform a LAN ID review to remove or disable all unused accounts. Going forward, HR should notify the LAN administrator upon employee terminations or transfers so that their access may be removed or changed in a timely manner.

MANAGEMENT ACTION

- *A process has been implemented whereby a 30 day audit will be performed on active LAN IDs.*
- *The Human Resources department already notifies the LAN Administrator of employee terminations or resignations. This process has recently been enhanced by implementing a process in which the exiting employee's supervisor reports this as well.*
- *Any changes reported will be acted on within 24 hours of notification.*

G. Daily Backups

Daily backup tapes are stored onsite in a non-fireproof rack. In the event of a fire or disaster affecting the building, the tapes stored in the cabinet would not be protected and the data would be lost, thereby impeding the company's ability to efficiently recover recent data.

RECOMMENDATION

Management should install a secure fireproof container for the storage of onsite back up tapes.

MANAGEMENT ACTION

The procurement of a suitably rated fire resistant storage unit has been implemented.

H. AIG Proprietary Message

The AIG proprietary message, which appears during initial logon to warn the user that the system belongs to AIG, is not active on all workstations. Without proper disclaimers for accessing AIG owned systems, it maybe difficult to prosecute an intruder in a court of law.

RECOMMENDATION

The LAN administrator should install proprietary messages on all user desktops.

MANAGEMENT ACTION

The proprietary message has now been installed on all user desktops.

VII. PASSWORD CONTROLS

A. Password Policy Settings

A review of the Windows NT account policy settings in Auto Warranty's' Primary Domain Controller (named LKMPRNT1) does not meet AIG password standards for the following areas:

- 'NT Password Minimum Age' is set to 0, allowing passwords to change immediately.
- 'Password Minimum Length' is set to 6 characters, while the AIG standard is 8.
- Password History is set to 5 passwords while the AIG standard is 13.
- NT password lockout duration is set to 15 minutes while the AIG standard is 60 minutes.

Not adhering to current standards does not provide appropriate security as directed by AIG management.

RECOMMENDATION

Management should implement current AIG password standards.

MANAGEMENT ACTION

All current standards set for NT account settings as stated above have been implemented.

B. A/EGIS Security

A review of A/EGIS user security administration disclosed that the application administrators in Maitland share a generic User-ID with a non-expiring password created by the ISG system support team to access the internet based security table. Generic user-IDs do not provide user accountability. Non-expiring passwords increases the possibility of unauthorized access.

RECOMMENDATION

The ISG A/EGIS support personnel should properly assign user-IDs that correspond to the users in Maitland and ensure passwords are changed regularly. Additionally, management should look into the feasibility of requesting a feature from ISG that will allow a user to change their password and force password expiration in A/EGIS.

MANAGEMENT ACTION

- *ISG will immediately create new User-IDs for the A/EGIS security administrators that correspond to the individual user.*
- *Additionally, ISG will prepare a time and cost estimate for implementing a user password forced change function with any non-compliant applications on-site and supply that to management.*

VIII. DISASTER AND BUSINESS RECOVERY

A review of disaster and business recovery disclosed that there is no formal DR and BCP plan. In the event of disaster, the lack of DR and BCP plan may impede the business from recovering in a timely and effective manner.

RECOMMENDATION

Management should develop and test a plan that includes but is not limited to the following:

- Documented procedures for restoring data and IT operations at an alternate location.
- The names of management personnel authorized to declare a disaster.
- Plans for relocating employees at alternate location or working from home.
- An inventory of data processing hardware and software.
- Daily and weekly operational procedures.
- List of IT vendor names with phone numbers and the products they represent.
- A section describing the backup tapes, specifically detailing the types of backups that exist, their location and access procedures to retrieve them.
- The plan should be distributed to key employees and a copy kept at the off-site location.

MANAGEMENT ACTION

We will continue with the investigation of developing a feasible DR and BCP plan for this business. Results as they become available will be presented to upper and executive management for plausibility.