

STATE OF NEW YORK INSURANCE DEPARTMENT  
REPORT ON EXAMINATION  
OF THE  
FARMERS & TRADERS LIFE INSURANCE COMPANY  
AS OF  
FEBRUARY 1, 2002

DATE OF REPORT:

FEBRUARY 1, 2002

EXAMINER:

ERNST & YOUNG LLP

## TABLE OF CONTENTS

<u>ITEM</u>		<u>PAGE NO.</u>
1.	Executive Summary	2
2.	Scope of Examination	3
3.	Description of Company	4
	A. History	4
	B. Company Operations	4
	C. Information Systems Department Organization	4
	D. Information Systems Environment	5
	E. Computer System Conversion	6
4.	Systems Overview	8
5.	Problem Management and Capacity Planning	11
6.	Change Management and Testing	13
7.	Logical and Physical Security	15
8.	Backup and Disaster Recovery	16
9.	Programming Errors and Problems	18
10.	Summary and Conclusions	20



STATE OF NEW YORK  
INSURANCE DEPARTMENT  
25 BEAVER STREET  
NEW YORK, NEW YORK 10004

February 1, 2002

Honorable Gregory V. Serio  
Superintendent of Insurance  
Albany, New York 12257

Sir:

In accordance with instructions contained in Appointment No. 21816, dated December 18, 2001 and annexed hereto, an examination has been made into the condition and affairs of Farmers & Traders Life Insurance Company, hereinafter referred to as "the Company," at its home office located at 960 James Street, Syracuse, New York 13203.

Wherever "Department" appears in this report, it refers to the State of New York Insurance Department.

The report indicating the results of this examination is respectfully submitted.

## 1. EXECUTIVE SUMMARY

The Company experienced significant information systems related problems with the implementation of its policy administration system. These problems were noted in item 8 of the Department's report on examination dated August 18, 2000. The purpose of this examination was to determine whether the information systems at the Company were adequately converted and remediated and that appropriate controls are in place with regard to the systems. The examiners found that many of the PolicyLink administration system processing errors and inefficiencies encountered after the application went into production in January 1997 have been remediated either through customization of the application or through manual work-arounds. From 1997 through 2001, the Company devoted significant attention and resources to get the system to process correctly, and meet the Company's needs with respect to its product portfolio.

This examination identified concerns with the Company's Information Systems ("IS") environment and related processes in the following areas:

- PolicyLink end user documentation
- Strategic IS plans
- IS policies and procedures
- IS problem management
- Application performance
- Application change management
- Application testing
- Logical security to the PolicyLink application
- Disaster and recovery planning

In addition, we found some PolicyLink processing errors and problems with the calculation of additional term insurance to be purchased on Extraordinary Life policies and the doubling of agent production credits.

## 2. SCOPE OF EXAMINATION

Ernst & Young, LLP (“E&Y”) was engaged by the Department to assist in the examination of the Company’s information systems. The examination’s objectives were to determine whether the existing information systems at the Company were adequately converted and remediated; and whether the systems satisfy and comply with New York Insurance Law and Department regulations, Company management policies and directives, and internal control standards deemed adequate by the Department. The examination also included reviewing the procedures implemented by the Company that address the comments contained in the Department’s report on examination dated August 18, 2000, related to information systems.

The examination included the following: review of the Company’s information systems policies, procedures, and available systems documentation; interviews with various business units, information systems and management personnel; limited tests of selected control processes; and review of Department information from the prior examination, the Company’s external auditor’s work papers, and various system-related management reports.

The examination addressed the following areas related to the development, maintenance, and processing of the PolicyLink and Freedom 2000 applications:

- System Overview
- Problem Management and Capacity Planning
- Change Management and Testing
- Logical and Physical Security
- Backup and Disaster Recovery
- Application Interfaces
- Suspense Reconciliation
- Programming Errors and Problems

In addition, the examination included a review of the processing and interface controls over the access database used for PolicyLink and Freedom 2000 suspense reconciliation (“Access Databases”), and the controls over the outsourcing of reserve data to Polysystems, a third party vendor.

### 3. DESCRIPTION OF COMPANY

#### A. History

The Company was incorporated as a stock life insurance Company under the laws of New York on July 3, 1912, was licensed, and commenced business on July 7, 1914, with the name Farmers National Insurance Company. The present name was adopted on September 17, 1914.

On October 8, 1953, the board of directors of the Company recommended a plan of mutualization of the Company pursuant to Section 199 of the New York Insurance Law (now Section 7302). The Company became a mutual life insurance company on December 20, 1974.

#### B. Company Operations

The Company currently does business in 28 states and sells its products through a sales agency force of about 1,600 agents. The portfolio of products includes whole life and term insurance, universal life insurance, and flexible and single premium deferred annuities. As of year-end 2001, the Company had about 66,000 policies with nearly \$2 billion of insurance coverage in force.

#### C. Information Systems Department Organization

The Company's IS Department consists of ten employees, divided into two areas: Applications and Operations. Both areas report to the Chief Actuary. There are three employees in Operations: an Operations Manager and two shift operators; and six employees in Applications: an Information Technology Director and five programmers.

The Operations area supports the Company's system operations environment. This comprises the hardware servers and local area network ("LAN") environment, the systems infrastructure, telecommunications network, system printers, desktop printers and approximately 100 workstations. The Operations area is responsible for the recovery of the Company's systems and computing environment in the event of a disaster. Operations personnel are also responsible for moving application program changes or enhancements into the production environment. In addition, the Operations area is responsible for user access security administration for both systems and applications.

The Applications area supports new product development and all PolicyLink application software program changes and enhancements. The Applications area is also responsible for maintaining and providing program support for the Access Databases. In addition, the Applications area is responsible for maintaining the PolicyLink extract application, which is used to provide reserve data to Polysystems, and for testing the vendor provided program changes for the Freedom 2000 application.

#### D. Information Systems Environment

The IS environment at the Company consists of three Novell 5.0 servers and a Microsoft Windows NT version 4.0 Lotus Notes server. Two Novell servers are used for the production environment and process the main production business applications in place at the Company. These applications are PolicyLink and Freedom 2000. PolicyLink is a Micro-Focus COBOL based application that is used to process and administer policy information. The Freedom 2000 application is used for the general ledger (statutory accounting), statutory reporting and accounts payable. The Company's programmers do not have access to the Freedom 2000 production code. Thus, the Company's programmers cannot make changes to the application's source code. The Freedom 2000 vendor provides all application code changes and software upgrades.

The Novell production servers are also used to allow Company employees to connect to the Internet. A firewall is in place between the Company's network and the Internet.

The third Novell server is called the Novell test environment server. This server contains actuarial data, reconciliation project data, the PolicyLink test area, and is used for IS backup/disaster server recovery testing. The actuarial data and reconciliation project data currently reside on the test server because there is not sufficient room on the production server to store this data. The Company plans to upgrade the Novell production servers during 2002. They will then migrate the actuarial data and reconciliation project data to the Novell production server during 2003.

The Novell LAN currently uses the Windows 95 and Windows 2000 operating systems. The Company is in the process of upgrading the LAN and workstations to the Windows 2000 operating system. This LAN is used as the front-end system to enable Company personnel to access the various applications on the Novell servers.

Novell network directory services (“NDS”) are used to authenticate users to the network. The PolicyLink and Freedom 2000 application security controls are used to control user access and functionality to these applications.

The NT and Novell production and test servers are backed up nightly onto tape using ArcServe software. The backup tapes are taken offsite the following business day.

#### E. Computer System Conversion

During 1994, the Company decided to convert from its former policy administration system, LifeComm, to the PolicyLink system. The PolicyLink system went into production on January 1, 1997. The PolicyLink system was formerly owned by the Leverage Group and is now owned by Computer Sciences Corporation (“CSC”).

Although PolicyLink was presented as an integrated administration system, there were serious shortcomings in its ability to support the Company’s portfolio of whole life, universal life, term, and fixed annuity products. Many customizations were performed after the application went into production to enable Policylink to meet the needs and requirements of the Company. Also in 1997, the Company upgraded to the Freedom 2000 general ledger system. The Freedom 2000 application was owned by the Freedom Group and was recently acquired by FISERV.

PolicyLink was not able to pass certain information to the Company’s Freedom 2000 general ledger system, which was needed to reconcile suspense accounts. As a result, a reconciliation application, using the Access Databases, was developed to facilitate the suspense reconciliation process. The Access Databases are also used to facilitate management reporting.

After the conversion to PolicyLink, the Company experienced policy related processing problems in producing information for management reporting, providing policyholder information, and calculating reserves, dividends and commissions. Many of these problems were the result of the inability of the PolicyLink application to meet the Company’s business needs, and inadequate testing of the system and the changes made to the core application’s processing modules. There was no parallel testing performed, and other testing such as end-to-end, full user acceptance, quality assurance, and integrated testing was limited. In addition, end user training courses were not provided by the vendor, until the March/April 1997 timeframe, almost four months after the application went into production.

From 1997 through 2001, the Company devoted significant attention and resources to modify the system so that it would process correctly and meet the Company's needs with respect to its product portfolio. Many of the processing errors and application deficiencies were noted in the Department's report on examination dated August 2000.

During 1998, the Company's relationship with the Leverage Group ended, and it was the last year the Company retained a maintenance agreement with the Leverage Group. Since that time, the Company's Application group has been responsible for the application maintenance and programming needs.

In 1998, the Company decided to outsource the reserve calculations to Polysystems as PolicyLink was not able to perform complex reserve calculations.

#### 4. SYSTEMS OVERVIEW

The objective in the systems overview area was to gain an understanding of the PolicyLink and Freedom 2000 applications and the functionality of these applications; obtain an understanding of current system issues or problems, and reserves processing; and understand the roles and responsibilities of the Company's IS Department and how this area supports the needs of the business. The following outlines our findings and recommendations resulting from our systems overview review.

##### A. PolicyLink End User Documentation

PolicyLink end user manuals by line of business or department have not been developed. Such manuals would facilitate users in understanding the application's functions and capabilities. Also, these manuals could be used to facilitate training and would be available for business continuity purposes.

The original PolicyLink vendor manuals address systems functionality, such as file descriptions, operational considerations, system processing, batch processing, menu functionality, commission processing, disbursement subsystem and administration information. However, these manuals are very detailed and some areas do not pertain to the Company's business (e.g., equity based products) or the Company's use of PolicyLink (e.g., reserve processing).

Within the PolicyLink application, we found instances where users have updated user instruction information in a form memo or diary log. These updates are used to assist users with understanding how some of the processing functions of the PolicyLink application operate. However, these instruction notes do not address all user functionality and are not necessarily maintained in a controlled fashion.

We recommend that user manuals by line of business or department be developed to enable users to understand PolicyLink application functions in use by the Company. Copies of such documentation, once finalized and approved by management, should also be included in the business continuity documentation.

## B. Strategic Information Systems Plan

Company management has developed a “2005 Vision” reflecting highlights of the Company’s overall strategic business plan, and a sales marketing plan showing market focus and planned activities. However, a strategic IS plan has not been developed and documented. We met with management to gain an understanding of the IS Department’s strategies. The main focus of the IS Department is to continue to support the needs of the business. Also, IS will continue to enhance the PolicyLink application software code. In addition, IS will address the needs of the Sales and Marketing groups in getting new products into the system to facilitate the Company’s “go to market” strategies. They are also upgrading their NT LAN platform to Windows 2000 and deploying new desktop computers for the users.

In the absence of a formal IS strategic plan, it is difficult to assess whether IS expectations and results will be achieved.

We recommend that the IS department document their strategic plans and also that it be included as part of the overall strategic business plan. This will ensure that such strategies are in line with business needs and that progress can be tracked, monitored and measured.

## C. Information Systems Policies and Procedures

Certain IS policies and procedures have been developed. However, the policies and procedures are not well indexed or centrally maintained. Some policies and procedures contain inconsistent formats, and are not made easily available for employee use. Many of the policies and procedures have been documented in email format in the Operation Manager’s Lotus Notes database or in the Information Technology Director’s directory in Microsoft Word. Policies and procedures are indexed in response to the Company’s external auditors, Price Waterhouse Coopers (“PWC”), April 2000 report comments instead of by process area or subject matter (e.g., system change management, physical security, user access). Not all policies and procedures provided contained evidence of management approval by the officer-in-charge of the IS Department or the Management Committee.

In addition, policies and procedures need to be improved and documented for:

- 1) Application performance - to determine whether the application is meeting user processing expectations;
- 2) IS problem management - to report, track and resolve all application and system related problems;

- 3) Systems development – (i) to address future development efforts and ensure that new applications are designed, built, tested, documented and implemented in a controlled and consistent fashion, (ii) procedures to address business and regulatory requirements as well as end user training needs, (iii) major components of a system development life cycle include systems requirement/solution definition, design, build and test phases; and
- 4) Testing methodology – to address test plans, test management and various areas of a test strategy (such as end-to-end, integrated and parallel testing) to help ensure that testing is performed in a consistent and robust fashion.

We recommend that all IS policies and procedures be developed, documented, properly indexed, and maintained in a consistent and centralized fashion. IS policies and procedures should also be approved by senior management personnel, and be made available for periodic management review and use by Company personnel.

## 5. PROBLEM MANAGEMENT AND CAPACITY PLANNING

The objective of the problem management and capacity planning review was to gain an understanding of the controls in place over these processes and determine whether the controls provide reasonable assurance that effective problem management and capacity planning processes are in place. Examination procedures involved understanding the Company's problem management procedures; reviewing issues and customer complaint logs; and understanding how problems are reported, tracked and resolved. For capacity planning, the examination procedures involved understanding user needs and expectations, how systems and application performance are monitored, and system metrics (such as system availability, downtimes, and capacity levels). The following outlines the findings and recommendations resulting from the problem management and capacity planning review.

### A. Information Systems Problem Management

The problem management process to facilitate the capturing and resolution of all system and application related problems needs to be improved. There are instances where problems are not documented on a timely basis nor are they documented in an issues log.

The process in place for the Applications group to document an application problem necessitates the development of a work request (by users or programmers). We found evidence that these work requests may not be documented until several months after the problem is encountered. For example, a problem was found with substandard risk production credits in June 2001 and a work request has not been documented as of the date of this report. Another problem associated with production credits for first premium payments has recently been documented into a formal work request. According to IS personnel, this problem has been in existence since the application went into production in 1997.

The process in place for the Operations group to document a systems related problem necessitates recording problems on a help desk log or in emails that are stored in various Lotus Notes databases and folders owned by the Operations Manager. It should be noted that not all problems communicated verbally are documented on the help desk log or in emails.

Neither of the processes described above are considered very effective or efficient methods for monitoring problems or performing trend analysis.

We recommend that an IS problem management process be developed and centralized to capture and track all (applications, systems and operations) IS issues and problems. Also, the process should address the monitoring, tracking, escalation and resolution of all IS problems and include trend analysis. This process should be documented for Company personnel to follow.

#### B. Application Performance

There is a documented capacity planning procedure in place to monitor system performance. Batch processing start and end times, application job runs, and batch cycle abnormal terminations are recorded and reviewed by Operations to understand cycle times, completion times, and capacity metrics. Daily capacity checklists are used to track service and capacity levels. Capacity information is manually summarized on a periodic basis and used for systems capacity planning purposes.

However, there is no procedure in place to address application performance and monitoring (e.g., on line response times, times incurred in processing application queries and ad hoc reports). As the Company adds new products or makes system changes or enhancements, it could negatively impact application performance if such metrics are not known or maintained. Monitoring of application performance would help identify the impact early to allow for appropriate resolution.

The Company should consider developing an application performance and monitoring process if they add to the automated systems currently in production or make other significant changes to the processing environment. This will enable IS management to understand what the response times are for on line application processing, queries and ad hoc reports to facilitate end user needs.

## 6. CHANGE MANAGEMENT AND TESTING

The objective of the change management and testing review was to gain an understanding of the controls in place over these processes and determine whether the controls in place provide reasonable assurance that there is an effective change management process in place. The change management process should address the testing, review and authorization of changes before they are moved into the Company's production processing environment. The following outlines our findings and recommendations resulting from our change management and testing review.

### A. Application Change Management

An application change management and testing procedure has been documented. All application changes, fixes or enhancements are to be tested by the programmers in the test environment. Testing includes regression testing, but it is limited to the prior application cycle run. End user and IS management authorization is obtained for the changes. The change is scheduled and the use of change management software (Source Integrity) to facilitate the change from the test environment to the production environment is used. Source Integrity is also used for application version control.

Separation of responsibilities related to the updating of programs into the production environment is in place. The programmers submit the change and the operations staff are responsible for moving the change into the production-processing environment.

There is a management committee made up of business users and IS personnel that meet to determine the impact and priority level of the application changes, fixes or enhancements, and prioritization of pending work requests. The priority levels are indicated on the Company's "Work Request" report for most of the pending work requests.

Programmers have full access to application production data and directories. Such access could result in unauthorized or inadvertent changes to production programs and data that may go unnoticed or undetected. Changes to programs could also negatively impact application processing and the integrity of information if the change is not properly tested and authorized. The control concern related to programmers having full access to production data was also raised by PWC in their May 27, 1999 and April 2000 reports. Company management recognizes this risk, and has decided to accept the risk given the occasional need for such access, the relatively

small number of programmers, and the close supervision of their activities. Management indicated that access is needed as the PolicyLink architecture requires that users of the system have network level update rights to its data files to execute file rebuild utilities in the event indexes become corrupt, and to facilitate the run of data update scans as part of completing specific work requests.

A review of the “Outstanding Systems Work Request” report to determine the validity of pending work requests is not regularly performed. Currently, the report indicates 190 outstanding work requests of which 55 work requests are over two years old. Also, some of the work requests are not prioritized. In addition, understanding the implementation period or estimated time to complete the work request is not documented.

The testing procedure only mentions regression testing and does not include a testing methodology or robust testing process. Test plans to facilitate the testing process are not always developed or documented. Integrated testing, end-to-end testing and the use of controlled test data are not in place. Also, regression testing uses the Monday cycle-run, which includes three days of activities, for testing purposes; however, this may not contain all transaction types to fully test the effect of all changes.

We recommend that management review with the Audit Committee the risks associated with programmers having full access to production data and program directories, and managements’ decision to accept such risks. A process should be put in place to review programmer access levels with the Audit Committee on an annual basis. Also, we recommend that work request development timeframes and the estimated time to complete the work request be developed and documented. A procedure should be developed to periodically review the work requests with business unit and senior management to substantiate and validate whether the work request is still required and that all are appropriately prioritized. A testing methodology should be developed to facilitate application testing and it should include integrated testing, end-to-end testing, and the use of controlled test data.

## 7. LOGICAL AND PHYSICAL SECURITY

The objective of the logical and physical security review was to gain an understanding of the controls in place over the PolicyLink and Freedom 2000 applications and the data center. Controls and procedures in place over user access and functionality to PolicyLink and Freedom 2000 were reviewed. Also, controls in place over physical access to the data center were reviewed to determine whether the data center was physically protected. The following outlines our findings and recommendations resulting from our logical and physical security review.

### A. PolicyLink Logical Security

User access rights to the PolicyLink system are not being properly maintained or kept current with the users current job responsibilities in accordance with the Company's documented logical security procedures. Many users on the PolicyLink system have more functionality than required. Company management is in the process of reviewing the PolicyLink access rights and working with IS to remove unwarranted access or access that is not consistent with the users' current job responsibilities.

We recommend that the Company complete its review of all user access and functionality in a timely manner to ensure that it is in alignment with the users' job responsibilities.

## 8. BACKUP AND DISASTER RECOVERY

The objective of the backup and disaster recovery review was to gain an understanding of the controls in place and determine whether such controls provide reasonable assurance that data, systems and operations can be successfully recovered and be available to users. Also, a business continuity plan should be in place to reasonably ensure that the recovery of critical business processes could take place in the event of a disaster. The following outlines our findings and recommendations resulting from our backup and disaster recovery review.

### A. Information Systems Disaster Recovery Plan

There is a documented IS disaster recovery memo that addresses the steps for server recovery. However, a comprehensive IS disaster recovery plan does not exist. The IS disaster recovery memo does not address a recovery site, testing, vendor information, emergency contact names and numbers, disaster declaration approval, and the recovery of all hardware/software components that IS is responsible for maintaining (such as system printers and telecommunications/PBX voice systems). An emergency disaster site for the processing of operations or a relocation vendor to assist with quickly finding an alternate processing site has not been defined.

Operations management has indicated that server restorations have been performed periodically using offsite tape backups to restore the server. However, test results and server recoverability timeframes are not retained.

We recommend that the Company develop a comprehensive IS disaster recovery plan. Such a plan should address hardware and system recovery, data retrieval procedures, emergency contact information, hardware/software vendor information, telecommunications recovery procedures, disaster declaration approval procedures, and physical recovery location. This plan should contain provisions to ensure periodical testing. The test plan and results (indicating problems found or successful completions) and indication of management approval should be maintained. The IS disaster recovery plan should be aligned with the business continuity plans, approved, and periodically reviewed by management to ensure it is meeting the needs of the business.

## B. Business Continuity Plan

The development and documentation of a business continuity plan is currently in progress. According to the Company, the business continuity plan is 60% complete and the Company expects the plan to be completed during 2002. The plan should identify the recovery of critical business processes. The plan should also identify supporting IS applications, vendors that would assist with locating alternate processing and office site locations, forms and documentation arrangements, network and application restoration procedures, and procedures to be followed by Company personnel during the disaster and recovery period.

We recommend the Company continue with the development and completion of its business continuity plan. We recommend once the business continuity plan is established that it be approved by management, tested and periodically reviewed to ensure it meets the needs of the business.

## 9. PROGRAMMING ERRORS AND PROBLEMS

The objective of the programming errors and problems review was to understand whether the controls in place provide reasonable assurance that the data inconsistencies, reported in the Department's report on examination dated August 2000, have been remediated. We found that many of the PolicyLink processing errors encountered after the application went into production in January 1997 have been remediated either through customization of the application or manual work-around, and various controls have been implemented.

As part of our examination, we also reviewed the processing and interface controls over the access database used for PolicyLink and Freedom 2000 suspense reconciliation, and the controls over the outsourcing of reserve data to Polysystems, a third party vendor. There were no control concerns identified in these areas.

During the review, certain PolicyLink processing errors relating to Extraordinary Life ("EOL") policies and agent production credits were identified. The following outlines our findings and recommendations resulting from our programming errors and problems review.

### A. Extraordinary Life

EOL policies involve the use of dividends to purchase a combination of term insurance and paid up additions to offset planned reductions in the policy's original face amount. The purpose is to reduce the premium outlay over the lifetime of the policy. This is described in the EOL policy plans.

During the review of the PolicyLink application, it was noted that PolicyLink was incorrectly calculating the amounts of term insurance and paid up additions to be purchased on the EOL policies. Specifically, the error resulted in excess term insurance being purchased. This error goes back to 1997 and was found in three of the four EOL plans affecting 951 policies. This issue was brought to the attention of the Company's management, who was aware of the problem but thought it had been corrected. A work request is currently being developed to address processing error.

However, the Company still needs to determine the total impact for the EOL policies in force as well as those EOL policies that have lapsed and surrendered. With respect to any EOL

death claims that have been processed, the beneficiaries may have received a greater benefit than planned. The Company has indicated that it will not seek to recoup any overpayments.

We recommend that the Company address the EOL processing errors for the three plans. The Company should complete its review to determine the impact of the EOL processing error and develop a plan of action to address in force as well as lapsed and surrendered policies.

#### B. Agent Production Credits

The “undo/redo” function for first premium payments when the policy date is not equal to the effective date is not functioning properly in the PolicyLink application, causing agent production credits to double.

When a payment is applied for a newly issued policy and the effective date of the payment is not equal to the policy effective date, or the policy date and the payment go through an “undo” process, the production credit is not reversed. When the next payment is processed, an additional production credit is created causing the agent's production credit to double. This error appears to date back to 1997 however a work request was not developed until January 2002.

Another problem found with production credits was with substandard risks. The agents were receiving double production credits. This error was first discovered in June 2001, however a work request has not been documented.

Subsequent to discovering the problem, the Company documented a procedure, which involves scanning the PolicyLink file extracts for certain events to prevent double production credits to agents.

While the manual work-around procedures should identify double credits, we recommend that the Company take the appropriate steps to correct the production credit errors.

## 10. SUMMARY AND CONCLUSIONS

The following are the findings and recommendations contained in this report:

<u>ITEM</u>	<u>DESCRIPTION</u>	<u>PAGE NO.</u>
A	We recommend that user manuals by line of business or department be developed to enable users to understand PolicyLink application functions in use by the Company. Copies of such documentation, once finalized and approved by management, should also be included in the business continuity documentation.	8
B	We recommend that the IS department document their strategic plans and also that it be included as part of the overall strategic business plan.	9
C	We recommend that all IS policies and procedures be developed, documented, properly indexed, and maintained in a consistent and centralized fashion. IS policies and procedures should also be approved by senior management personnel, and be made available for periodic management review and use by Company personnel.	10
D	We recommend that an IS problem management process be developed and centralized to capture and track all (applications, systems and operations) IS issues and problems. Also, the process should address the monitoring, tracking, escalation and resolution of all IS problems and include trend analysis. This process should be documented for Company personnel to follow.	12
E	The Company should consider developing an application performance and monitoring process if they add to the automated systems currently in production or make other significant changes to the processing environment. This will enable IS management to understand what the response times are for on line application processing, queries and ad hoc reports to facilitate end user needs.	12
F	We recommend that management review with the Audit Committee the risks associated with programmers having full access to production data and program directories, and managements' decision to accept such risks. A process should be put in place to review programmer access levels with the Audit Committee on an annual basis.	14

<u>ITEM</u>	<u>DESCRIPTION</u>	<u>PAGE NO.</u>
G	We recommend that work request development timeframes and the estimated time to complete the work request be developed and documented. A procedure should be developed to periodically review the work requests with the business unit and senior management to substantiate and validate whether the work request is still required and that all are appropriately prioritized.	14
H	We recommend that a testing methodology be developed to facilitate application testing and it should include integrated testing, end-to-end testing, and the use of controlled test data.	14
I	We recommend that the Company complete its review of all user access and functionality in a timely manner to ensure that it is in alignment with the users' job responsibilities.	15
J	We recommend that the Company develop a comprehensive IS disaster recovery plan. Such a plan should address hardware and system recovery, data retrieval procedures, emergency contact information, hardware/software vendor information, telecommunications recovery procedures, disaster declaration approval procedures, and physical recovery location. This plan should contain provisions to ensure periodical testing. The test plan and results (indicating problems found or successful completions) and indication of management approval should be maintained. The IS disaster recovery plan should be aligned with the business continuity plans, approved, and periodically reviewed by management to ensure it is meeting the needs of the business.	16
K	We recommend the Company continue with the development and completion of its business continuity plan. We recommend that once the business continuity plan is established it be approved by management, tested and periodically reviewed to ensure it meets the needs of the business.	17

<u>ITEM</u>	<u>DESCRIPTION</u>	<u>PAGE NO.</u>
L	We recommend that the Company address the EOL processing errors for the three plans in which the incorrect amount of additional term insurance is being purchased. The Company should complete its review to determine the impact of the EOL processing error and develop a plan of action to address in force policies as well as lapsed and surrendered policies.	19
M	We recommend that the Company take the appropriate steps to correct the production credit errors.	19



APPOINTMENT NO. 21816

STATE OF NEW YORK  
**INSURANCE DEPARTMENT**

I, GREGORY V. SERIO, Superintendent of Insurance of the State of New York, pursuant to the provisions of the Insurance Law, do hereby appoint:

ERNST & YOUNG LLP

as a proper person to examine into the affairs of the

**FARMERS & TRADERS LIFE INSURANCE COMPANY**

and to make a report to me in writing of the condition of the said

**COMPANY**

with such other information as he shall deem requisite.

In Witness Whereof, I have hereunto subscribed by name  
and affixed the official Seal of the Department  
at the City of New York

this 18th day of December, 2001



GREGORY V. SERIO

Superintendent of Insurance

A handwritten signature in black ink, appearing to read "Gregory V. Serio", written over a horizontal line.

Superintendent