S. KEEHN REMARKS

INFORMATION SECURITY CONFERENCE

SEPTEMBER 10, 1987

I. WELCOME - GIVEN THE SIZE OF OUR AUDIENCE, AND THE NATURE OF REPRESENTATION, TOPIC OBVIOUSLY OF GREAT INTEREST AND IMPORTANCE.

A. TEN YEARS AGO, WE PROBABLY WOULDN'T HAVE HELD SUCH A MEETING.

1. THE NEED SIMPLY WASN'T THERE THEN - NOT TO SUGGEST THAT SECURITY WASN'T IMPORTANT - CERTAINLY IT WAS.

2. BUT RATHER, THE NATURE OF THE SECURITY PROBLEM WAS MUCH DIFFERENT.

3. SECURITY MEASURES WERE EASIER TO DEAL WITH - THEY WERE MUCH MORE STRAIGHT FORWARD.

4. TRADITIONAL SAFEKEEPING METHODS WERE QUITE ADEQUATE TO ASSURE ESSENTIAL PROTECTION.

B. THE DEVELOPMENT (READ REVOLUTION) OF ELECTRONICS HAS CHANGED ALL OF THAT AND HAS ASSAULTED TWO OF THE ABSOLUTELY ESSENTIAL ELEMENTS OF BANKING AND OTHER FINANCIAL SERVICES ENTITIES.

1. THE PROTECTION OF ASSETS.

2. MAINTAINING THE INTEGRITY AND ABSOLUTE CONFIDENTIALITY OF INFORMATION.

C. BEFORE THIS REVOLUTION, PROCEDURES COULD AND WERE DEVELOPED WHICH SAFEGUARDED THESE ESSENTIAL KEYSTONES.

1. THESE PROCEDURES, WHILE CERTAINLY NOT FAILSAFE, NONETHELESS PROVIDED A HIGH LEVEL OF ASSURANCE THAT VIOLATIONS COULD NOT BE EASILY ACCOMPLISHED AND COULD BE DETECTED.

D. BUT TO SAY THE OBVIOUS, THE WORLD IS VERY, VERY DIFFERENT NOW.

1. VIRTUALLY EVERYTHING, FINANCIAL RECORDS, DATA, INFORMATION, CORRESPONDENCE - ALL OF THE ITEMS OF EXTREME IMPORTANCE TO AN ORGANIZATION ARE MAINTAINED IN SOME TYPE OF ELECTRONIC MODE.

2. WITHOUT SPECIFIC CONTROLS AND MONITORING MECHANISMS

A. THESE RECORDS ARE NOW MORE ACCESSIBLE TO VIOLATION.

B. DETECTION IS HARDER.

C. IT CAN OCCUR ALMOST UNNOTICED.

II. THE RISKS HERE ARE, OF COURSE, ENORMOUS.

A. FIRST THERE IS THE RISK OF FINANCIAL LOSS.

1. THERE ARE ALL SORTS OF SCARE STORIES, AND WE'VE ALL HEARD THEM, WHICH CAN'T HELP BUT PUT MANAGEMENT ON THE EDGE OF ITS CHAIR.

2. SOME YEARS AGO IN A FORMER ORGANIZATION - AND I EMPHASIZE BEFORE I JOINED THE FEDERAL RESERVE BANK OF CHICAGO - I HAD SUCH AN EXPERIENCE.

3. I HAD THE MANAGEMENT RESPONSIBILITY FOR OPERATIONS AT A BANK WHERE A $1,000 WIRE TRANSFER WAS ERRONEOUSLY ESCALATED TO $1 MILLION, TRANSFERRED TO A FOREIGN DEPOSIT ACCOUNT AND THEN FRAUDULENTLY REMOVED FROM THE ACCOUNT AT THE OTHER END.

4. NOT ONLY DID WE EXPERIENCE THE FINANCIAL LOSS BUT THE ATTENDANT PUBLICITY WAS EXCRUCIATING AND PREDICTABLY THE RESULTING LEGAL FEES AND OTHER EXPENSES WERE ALMOST AS HIGH AS THE LOSS OF THE TRANSFER.

B. OTHER THAN THE FINANCIAL LOSS THERE IS THE SERIOUS RISK THAT INVOLVES THE INTRUSION INTO HIGHLY CONFIDENTIAL DATA OR INFORMATION.

1. ALL ORGANIZATIONS POSSESS DATA AND INFORMATION THAT IS OF UTMOST IMPORTANCE TO THEIR PARTICULAR INSTITUTION. WHEN IT WAS MANUALLY MAINTAINED, IT COULD EASILY BE PLACED IN A FILE DRAWER, PERHAPS UNDER DUAL CONTROL. INTEGRITY WAS PRETTY GOOD.

2. BUT NOW THAT IT IS STORED ELECTRONICALLY, ACCESS IS A DIFFERENT QUESTION.

C. INTRUSION THAT INVOLVES EITHER OF THESE RISKS, FINANCIAL LOSS AND/OR EXPOSURE OF CONFIDENTIAL INFORMATION, EFFECTS THE CONFIDENCE IN AND INTEGRITY OF THE PARTICULAR INSTITUTION AND CAN RESULT IN PRETTY AWKWARD EMBARRASSMENT.

D. HARDLY A DAY GOES BY THAT I DON'T WORRY THAT SOMEONE OUT THERE (OR EVEN WORSE SOMEONE WITHIN OUR OWN INSTITUTION) IS WORKING AWAY AT A PLAN TO VIOLATE OUR SAFEGUARD PROCEDURES AND GAIN ACCESS TO FINANCIAL ASSETS OR INFORMATION.

1. MAJOR FINANCIAL INSTITUTIONS FIRST HAVE TO REPRESENT AN IRRESISTIBLE TARGET FOR THESE KINDS OF PEOPLE.

E. SOMEHOW THIS SEEMS TO HAVE BEEN AN ISSUE THAT HAS RATHER CREPT UP ON US.

1. IN FORMER DAYS, AS I SUGGESTED, SECURITY ISSUES HAD A DIFFERENT DIMENSION.

A. SAFEGUARD PROCEDURES WERE DEVELOPED, PUT IN PLACE AND AUDIT CHECKS ASSURED ADHERENCE.

B. SENIOR MANAGEMENT, THEREFORE, DID NOT NEED TO BE INVOLVED ON A DAY-TO-DAY BASIS.

2. BUT ELECTRONICS, OF COURSE, HAVE CHANGED THIS. ACCESS ISSUES ARE ENTIRELY DIFFERENT.

A. SENIOR MANAGEMENT MUST BE INVOLVED; CLEARLY THIS IS AN IMPORTANT MANAGEMENT ISSUE.

B. AND IT IS ONE THAT MUST RECEIVE OUR CONTINUING ATTENTION.

III. THE RATE OF TECHNOLOGICAL CHANGE IS QUITE INCREDIBLE.

A. PROCEDURES THAT WERE APPROPRIATE LAST YEAR MAY NOT BE TODAY AND CERTAINLY WON'T BE TOMORROW.

B. THE VOLUMES AND VELOCITIES HAVE GOTTEN VERY, VERY LARGE - AND RAPIDLY.

1. AT OUR BANK LAST YEAR, ALMOST $21 TRILLION IN FUNDS WERE TRANSFERRED OVER THE FEDERAL WIRE.

2. THE AVERAGE TRANSACTION WAS $9.2 MILLION.

3. ON A BROADER SCALE, IT IS ESTIMATED THAT THE DAILY VALUE OF TRANSFERS ON FEDERAL WIRES IS ABOUT $1 TRILLION.

IS EXPONENTIALLY INCREASED.

C. WHILE THESE NUMBERS ARE GROWING AT A STAGGERING RATE, THERE IS ANOTHER IMPORTANT, BUT MORE SUBTLE SHIFT TAKING PLACE.

1. HERETOFORE THE ELECTRONICS WORLD HAS LARGELY BEEN IN THE WHOLESALE DOMAIN; COMMERCIAL BANKS, CORPORATIONS AND THE LIKE.

2. INCREASINGLY THOUGH, ELECTRONIC ACTIVITY IS GROWING AT THE RETAIL LEVEL.

3. WITH THIS PROLIFERATION, THE OPPORTUNITY FOR SECURITY VIOLATIONS IS EXPONENTIALLY INCREASED.

D. AT THE WHOLSESALE LEVEL, WHILE IN THE PAST BANKS HAVE BEEN ABLE TO MONITOR AND ESSENTIALLY CONTROL TRANSACTIONS BETWEEN TWO ENTITIES, ONE CAN IMAGINE THE EXTENSION OF THIS PROCESS RESULTING IN THE BANKS MERELY SERVING AS THE CONDUIT THROUGH WHICH TRANSACTIONS ARE AUTOMATICALLY PROCESSED. WITH A LITTLE IMAGINATION, THIS POSES SOME RATHER SCARRY POSSIBILITIES AND RAISES THE DIFFICULT QUESTION AS TO JUST WHO WILL BEAR THE ULTIMATE RESPONSIBILITY IN THIS PROCESS.

IV. NEARER AT HAND, THE DEREGULATION OF THE FINANCIAL INDUSTRY HAS RESULTED IN THE PROLIFERATION OF NEW PRODUCTS AND SERVICES WHICH DEPEND ON COMPLEX COMPUTER SYSTEMS FOR PRODUCTION OR DELIVERY. TECHNOLOGICAL ADVANCEMENTS HAVE ALSO MADE IT POSSIBLE FOR FINANCIAL INSTITUTIONS TO OFFER SOPHISTICATED INFORMATION SERVICES TO THEIR CUSTOMERS. SINCE MORE AND MORE ORGANIZATIONAL FUNCTIONS ARE BEING ENTRUSTED TO COMPUTERS AND THEIR SUPPORTING

COMMUNICATIONS NETWORKS, IT IS ESSENTIAL THAT FINANCIAL INSTITUTIONS DEVELOP SOUND CONTROLS FOR COORDINATING AND INTEGRATING OPERATIONS AND AUTOMATION.

AS THE FINANCIAL SYSTEM BECOMES MORE ELECTRONIC, MORE COMPLEX, AND MORE INTERNATIONAL, THESE CONTROLS WILL BECOME ABSOLUTELY IMPERATIVE. WITH TODAY'S 24-HOUR GLOBAL BANKING AND TRADING MARKETS, MONEY CAN BE ELECTRONICALLY TRANSMITTED THROUGH MANY ACCOUNTS IN SEVERAL COUNTRIES IN A MATTER OF MINUTES. THE IRAN-CONTRA HEARINGS HIGHLIGHTED SOME OF THE DIFFICULTIES INVOLVED IN ESTABLISHING AN AUDIT TRAIL FOR SUCH COMPLEX GLOBAL TRANSACTIONS.

V. GIVEN THE NATURE OF THE FEDERAL RESERVE SYSTEM'S RESPONSIBILITIES - OUR CENTRAL BANK ROLE - WE HAVE BEEN ACUTELY AWARE OF THE NEED FOR SAFEGUARDS IN THE ELECTRONIC AREA.

A. WE LIKE TO THINK THAT WE HAVE BEEN ON THE LEADING EDGE ON THIS.

2. DATA ENCRYPTION FOR COMPUTER LINKS AND THE IMPLEMENTATION OF CONTROLS ON PERSONAL COMPUTERS AND ATTENTION TO DATA CLASSIFICATIONS ARE ONLY PART OF OUR ONGOING PROGRAM TO ENSURE A SECURE ENVIRONMENT FOR OUR CUSTOMERS AND FOR OURSELVES.

VI. NOT ONLY HAS THE ENVIRONMENT CHANGED DRAMATICALLY BUT THE SOURCE OF THE PROBLEM HAS ALSO CHANGED - AND I FIND IT AN AWKWARD SHIFT.

A. AS THE ELECTRONIC WORLD DEVELOPED, MANAGERS WERE CONCERNED WITH PREVENTING VIOLATION FROM EXTERNAL SOURCES.

1. AND THIS, OF COURSE, CONTINUES TO BE A CRITICAL ISSUE.

B. BUT LATER, IT WAS DISCOVERED THAT THE MAIN SOURCE OF SECURITY PROBLEMS IS NOT OUTSIDERS BUT INSIDERS.

1. EMPLOYEE ERRORS, OMISSIONS, FRAUD AND EMBEZZLEMENT ACCOUNT FOR MORE THAN HALF OF ALL ELECTRONIC SECURITY PROBLEMS.

2. IN A RECENT CASE OF INSIDER FRAUD AT A BANK, A WELL-RESPECTED SENIOR TECHNICAL OFFICER OPENED UNAUTHORIZED ACCOUNTS IN THE BANK'S COMPUTER RECORDS. HE USED THESE FICTITIOUS ACCOUNTS TO STEAL OVER $1 MILLION. IRONICALLY, THE PERPETRATOR WAS EVENTUALLY CAUGHT AS A RESULT OF AN IMPROPERLY FUNCTIONING ADDRESS MACHINE. ELECTRONIC FRAUD CAUGHT BY A SIMPLE MECHANICAL MALFUNCTION. TWO OF THE CHECKS DRAWN ON THESE FICTITIOUS ACCOUNTS AND SENT TO A FICTITIOUS ACCOUNT HOLDER WERE RETURNED TO THE BANK BECAUSE OF INSUFFICIENT ADDRESS INFORMATION. THE RETURNED CHECKS WERE INVESTIGATED BY THE CUSTOMER SERVICE SECTION, WHICH DETECTED AN IRREGULARITY. THE AUDIT DEPARTMENT WAS CONTACTED, AND AFTER A SERIES OF INVESTIGATIONS THE PERPETRATOR WAS FINALLY APPREHENDED. HE RETURNED THE UNSPENT PORTION OF THE STOLEN MONEY, WHICH HAD BEEN REDUCED TO ABOUT ONE-HALF OF THE ORIGINAL AMOUNT.

3. MANAGERS HAVE NOT ONLY COME TO REALIZE THAT EMPLOYEES POSE THE GREATEST THREAT TO SECURITY, BUT THEY HAVE ALSO DISCOVERED THAT THE INTRODUCTION OF NEW SECURITY TECHNOLOGIES FREQUENTLY REQUIRE THE ESTABLISHMENT OF NEW

PROCEDURES FOR MANAGING EMPLOYEES. FOR EXAMPLE, THE VERY DESIGN OF SOPHISTICATED ACCESS CONTROL SYSTEMS REQUIRED DATA OWNERS TO TAKE RESPONSIBILITY FOR DECIDING WHO WOULD HAVE ACCESS TO THEIR DATA AS WELL AS WHEN, HOW MUCH, AND WHAT TYPE OF ACCESS WOULD BE ALLOWED. MANAGEMENT PROCEDURES HAD TO BE DEVELOPED TO CONTROL THE ACCESS OF STAFF MEMBERS TO INFORMATION SYSTEMS, AUDIT TRAILS HAD TO BE ESTABLISHED TO ENSURE THAT PASSWORDS WERE TIGHTLY CONTROLLED, AND STAFF DUTIES HAD TO BE SEPARATED SO THAT NO ONE PERSON HAD COMPLETE ACCESS TO ANY ONE INFORMATION SYSTEM. IN OTHER WORDS, MANAGEMENT HAD TO DEVELOP CONTROLS COVERING THE ENTIRE INFORMATION LIFE CYCLE FROM THE CREATION OF THE INFORMATION, TO ITS TRANSFORMATION INTO AUTOMATED DATA, TO ITS VARIOUS USES, TO ITS FINAL UTILIZATION, STORAGE OR DESTRUCTION.

VII. WITH THAT BY WAY OF BACKGROUND, LET ME NOW QUICKLY HIGHLIGHT SOME OF THE KEY ISSUES THAT WILL BE ADDRESSED IN GREATER DETAIL THROUGHOUT OUR CONFERENCE. ~~THESE INCLUDE:~~ Associates have put together an excellent agenda and assembled an outstanding group of speakers.

- MICROCOMPUTER SECURITY

- SECURITY MANDATES

- FEDERAL GOVERNMENT INVOLVEMENT

- FEDERAL RESERVE ASSISTANCE AND SOLUTIONS

- IMPLEMENTING A SECURITY PROGRAM

VIII. FIRST, MICROCOMPUTER SECURITY

A. THE ADVENT OF THE MICROCOMPUTER HAS MADE IT POSSIBLE FOR ORGANIZATIONS OF ALL TYPES AND SIZES TO REAP THE BENEFITS OF COMPUTER POWER. BUT THE GROWING USE OF MICROCOMPUTERS HAS ALSO CREATED NEW SECURITY RISKS, AND MANAGERS HAVE HAD TO DEVELOP CONTROLS TO PROTECT THESE NEW AND HIGHLY FLEXIBLE INFORMATION SYSTEMS. MANAGERS CAN NO LONGER RELY SOLELY ON THE PHYSICAL AND PROCEDURAL SAFEGUARDS DESIGNED TO PROTECT THE EQUIPMENT, SOFTWARE AND INFORMATION HOUSED IN A CENTRAL COMPUTER FACILITY.

THE SECURITY REQUIREMENTS FOR MICROCOMPUTERS DIFFER SUBSTANTIALLY FROM THOSE OF A CENTRAL COMPUTER FACILITY BECAUSE MICROCOMPUTERS ARE USUALLY WIDELY DISPERSED THROUGHOUT AN ORGANIZATION. EQUIPMENT, PROGRAMMING, PROCESSING, AND

DATA/SOFTWARE STORAGE ARE ALL DECENTRALIZED. AS A RESULT, THE DATA PROCESSING DEPARTMENT OF AN ORGANIZATION NO LONGER HAS TOTAL CONTROL OVER DATA SECURITY AND NEW CONTROLS HAVE TO BE ESTABLISHED TO ENSURE DATA INTEGRITY.

IX. THEN SECURITY MANDATES

A. IN THE FORESEEABLE FUTURE, FEDERAL AND STATE LAWS, PROFESSIONAL STANDARDS, AND INSURANCE GUIDELINES WILL TEND TO PROMOTE MANDATORY, RATHER THAN VOLUNTARY, SECURITY PRACTICES. ALREADY, SOME CORPORATIONS ARE REQUIRED TO ENFORCE SPECIFIC SECURITY PROCEDURES. FINANCIAL INSTITUTIONS USING MICROCOMPUTERS TO FUNCTION ELECTRONIC TRANSACTIONS THROUGH THE FEDERAL RESERVE SYSTEM ARE REQUIRED TO ENCRYPT THEIR TRANSACTIONS. CONTRACTORS WITH THE DEPARTMENT OF DEFENSE ARE REQUIRED TO FILE A RISK ANALYSIS PLAN FOR PROTECTING INFORMATION RESOURCES ASSOCIATED WITH THEIR CONTRACTS. ALSO, COMPANIES USING PURCHASED SOFTWARE MUST INSTITUTE A SECURITY AWARENESS PROGRAM TO ENSURE THAT THEY WILL NOT BE SUED FOR UNAUTHORIZED DUPLICATION OF THE SOFTWARE.

X. AND THERE IS THE QUESTION OF FEDERAL GOVERNMENT INVOLVEMENT

A. THE FEDERAL GOVERNMENT HAS TAKEN AN ACTIVE ROLE IN PROMOTING INFORMATION SECURITY IN THE FINANCIAL INDUSTRY. THE NATIONAL SECURITY AGENCY IS CONDUCTING EXTENSIVE TESTS OF MAINFRAME

COMPUTERS AND HAS DEVELOPED GUIDELINES ON HOW TO SELECT MAINFRAMES. THE NATIONAL BUREAU OF STANDARDS' INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY IS ESTABLISHING SECURITY STANDARDS FOR MICROCOMPUTER SYSTEMS. AT THE DEPARTMENT OF THE TREASURY, STANDARDS ARE BEING DEVELOPED FOR MESSAGE AUTHENTICATION. AND AT THE DEPARTMENT OF DEFENSE'S COMPUTER INSTITUTE, SECURITY TRAINING PROGRAMS ARE CONDUCTED FOR ALL FEDERAL AGENCIES.

XI. WITH REGARD TO FEDERAL RESERVE ASSISTANCE AND SOLUTIONS

A. IN RECENT YEARS, THE FEDERAL RESERVE SYSTEM HAS ALSO BECOME ACTIVE IN PROMOTING INFORMATION SECURITY. CURRENTLY, SYSTEMWIDE SECURITY STANDARDS ARE BEING DEVELOPED FOR ALL FORMS OF INFORMATION MEDIA. IN CONJUNCTION WITH THESE SYSTEMWIDE EFFORTS, THE CHICAGO RESERVE BANK WILL BE PROVIDING A VARIETY OF EDUCATIONAL PROGRAMS TO ASSIST FINANCIAL INSTITUTIONS IN MEETING THEIR SECURITY NEEDS AND TO ENSURE THE INTEGRITY OF THE NATION'S PAYMENTS MECHANISMS.

XII. FINALLY AND OF CRITICAL IMPORTANCE, IMPLEMENTING A SECURITY PROGRAM

A. IN RESPONSE TO MANAGEMENT INTEREST IN INFORMATION SECURITY AND TO GOVERNMENTAL, PROFESSIONAL AND INDUSTRY PRESSURES TO IMPROVE INFORMATION SECURITY, MANY FINANCIAL INSTITUTIONS HAVE IMPLEMENTED, OR ARE BEGINNING TO IMPLEMENT, INFORMATION

SECURITY PROGRAMS. AS A BAREBONES OUTLINE OF AN APPROPRIATE PROGRAM, WE SUGGEST THAT FINANCIAL INSTITUTIONS TAKE AT LEAST FOUR STEPS:

1. ASSIGN RESPONSIBILITY FOR INFORMATION SECURITY.

2. INCORPORATE INFORMATION SECURITY INTO THEIR STRATEGIC PLANS.

3. ESTABLISH A CORPORATE SECURITY POLICY.

4. START AN ORGANIZATIONWIDE SECURITY AWARENESS PROGRAM TO INFORM INFORMATION SYSTEM USERS ABOUT THE SECURITY RULES THAT WILL AFFECT THEM.

XIII. TO CONCLUDE

A. IT IS CLEAR THAT INFORMATION AND ELECTRONICS SECURITY HAS BECOME AND WILL CONTINUE TO BE AN IMPORTANT MANAGEMENT PRIORITY FOR FINANCIAL INSTITUTIONS. IN THE FUTURE, SECURITY CONSIDERATIONS WILL INFLUENCE THE WAY ORGANIZATIONS ARE STRUCTURED AND, MORE GENERALLY, THE WAY WORK IS PERFORMED. EFFECTIVE INFORMATION SECURITY WILL REQUIRE A COMBINATION OF SOUND MANAGERIAL PRACTICES AND STATE-OF-THE-ART SECURITY TECHNOLOGIES. WE WILL ALL NEED TO WORK TOGETHER TO PROTECT THE INFORMATION ASSETS OF OUR INDUSTRY. I BELIEVE THAT THIS CONFERENCE WILL SERVE AS A MAJOR STEP FORWARD IN THIS COOOPERATIVE EFFORT.

1. WHILE, AS I SUGGESTED AT THE OUTSET, TEN YEARS AGO THIS MEETING MIGHT NOT HAVE BEEN NECESSARY, IT CERTAINLY IS TODAY AND WE ARE DELIGHTED TO HOST IT.

THANK YOU.