THE INTERNATIONAL HANDBOOK ON COMPUTER CRIME

Ulrich Sieber

The International Handbook on Computer Crime

Computer-related Economic Crime and the Infringements of Privacy

Ulrich Sieber

Institute of Criminology and Economic Criminal Law, University of Freiburg,
Federal Republic of Germany

JOHN WILEY & SONS
Chichester · New York · Brisbane · Toronto · Singapore

***Library of Congress Cataloging-in-Publication Data*:**

Sieber, Ulrich, Dr.
The international handbook on computer crime.

Bibliography: p.
Includes index.
1. Computer crimes. 2. Computers—Access control.
I. Title.
HV6773.S54 1986 364.1′68 86-15670
ISBN 0 471 91224 7

***British Library Cataloguing Data*:**

Sieber, Ulrich
The international handbook on computer crime
1. Computer crimes
I. Title
364.1′62 HV6773

ISBN 0 471 91224 7

Typeset by Inforum Ltd, Portsmouth
Printed and bound in Great Britain

Preface and Acknowledgements

Computer crime has become a subject of international concern in recent years due to worldwide advances in computers, close international co-operation in data processing, and an increasing transnational data flow via international communications networks. Consequently, fighting computer crime cannot be continued at a national level but must be extended by close international co-operation, especially in the fields of criminological research, clarification and reform of prevailing legal provisions, development of security measures, and prosecution of computer crime.

This book is intended to initiate this international effort. The author's German books, *Computerkriminalität und Strafrecht* (2nd edn, 1980) and *Informationstechnologie und Strafrechtsreform* (1985), provide a detailed criminological analysis of computer-related economic crime and respective West German law. In contrast, this book is extended to an international overview of all kinds of computer crime, a comparative analysis of the legal situation in major Western countries, a presentation of the most important security measures discussed at an international level, as well as an analysis of problems arising in the field of prosecution.

The work presented in this book is based on a continuing study of the field of computer-related crime and information law which the author has been carrying out at the Institute of Criminology and Economic Criminal Law at the University of Freiburg in close co-operation with research institutes in other countries since 1974. The book is also founded on the author's work as an attorney in the field of information law and as a lecturer in computer crime and computer security. The international legal aspects of the study originate from his work as a consultant for the Organization for Economic Co-operation and Development (OECD) in Paris, for which he prepared a comparative legal study which became the basis of section IV.A. Analysis of the international aspects has also been supported by his activities as a member of the Legal Observatory for the Community Information Market of the Commission of the European Communities and as a scientific member of the Select Committee of Experts on Computer-related Crime of the Council of Europe, for which he prepared a draft study which became the basis of subsection IV.A.2c and Section IV.B.

As the issue of computer crime is a most topical one and subject to very rapid changes, work in this field can only be carried out in close co-operation with researchers in several countries. Consequently this study is based not only on the author's work but is also the result of many contributions by friends and colleagues. It is not possible to mention all who have contributed to this research. However, the author would especially like to thank for their help Mr Jay Bloombecker (Los Angeles), Professor Dr Pierre-Henri Bolle (Neuchâtel), Ms Martine Briat (Paris), Professor Dr Jean Cosson (Paris), Mr Kevin J. Fitzgerald (East Malvern/Australia), Ms Michèle Franke (Montreal), Mr Hans-Peter Gassmann (Paris), Professor Dr Nico Keijzer (Amsterdam), Mr Paul Kenneth (Paris), Mr Manfred Kindermann (Böblingen), Mr Lauri Lehtimaja (Helsinki), Mr John F. Ley (Barton/Australia), Professor Dr Jaime Malamud-Goti (Buenos Aires), Mr Finn Meilby (Copenhagen), Dr Manfred Möhrenschlager (Bonn), Professor Dr Fermin Morales Prats (Barcelona), Mr. C.G.B. Nicholson (Edinburgh), Professor Dr Norıyuki Nishida (Tokyo), Mr Donn B. Parker (Menlo Park), Ms Betina Pasquali (Buenos Aires), Mr Alexander Patijn (Amsterdam), Dr Lorenzo Picotti (Bologna), Mr Donald K. Piragoff (Ottawa), Ms Charlotte M. Pitrat (Paris), Dr Carlo Sarzana (Rome), Mr Stein Schjolberg (Oslo), Dr Gabriele Schmölzer (Innsbruck), Professor Dr Bart de Schutter (Brussels), Mr Artur Solarz (Stockholm), Professor Dr Dionysios Spinellis (Athens), Mr Erik Tersmeden (Stockholm), Professor Dr Guy P.V. Vandenberghe (Amsterdam), Dr Ken Wong (Manchester), and Dr Erwin Zimmerli (Zurich). Above all, the author is most grateful to his academic mentor, Professor Dr Dr Klaus Tiedemann (Freiburg i. Br.), for his constant support.

An international analysis of a new and quickly changing phenomenon will hardly be without omissions. All deficiencies of the present study fall uniquely within the author's responsibility. The author would like to apologize to all researchers whose works might have been overlooked. He would appreciate being informed of their research and thus having them participate in the international co-operation which is intended by the present publication.

Ulrich Sieber
Freiburg i.Br., March 1986

Contents

Preface and Acknowledgements xiii

I. INTRODUCTION: THE EMERGENCE OF A NEW THREAT 1

II. THE PHENOMENA OF COMPUTER CRIME 3

A. Computer-related Economic Crimes 3

1. Fraud by Computer Manipulation 3
   a. Objects of Computer-related Fraud 4
   b. *Modi Operandi:* The Methods of Manipulation 6
   c. Perpetrators 11
2. Computer Espionage and Software Piracy 12
   a. Objects of Espionage 12
   b. *Modi Operandi* 13
   c. Perpetrators 14
3. Computer Sabotage 15
   a. Objects of Sabotage 15
   b. *Modi Operandi* 15
   c. Perpetrators 17
4. Theft of Services 18
5. Unauthorized Access to DP Systems and 'Hacking' 19
6. The Computer as a Tool for Traditional Business Offences 20

B. Computer-related Infringements of Privacy 21

1. Use of Incorrect Data 21
   a. Manipulation and Erasure of Personal Data by Unauthorized Persons 22
   b. Collection, Processing, and Dissemination of Incorrect Data by their Legitimate Holder 22
2. Illegal Collection and Storage of Correct Data 23
   a. Illegal Techniques of Obtaining Data 23
   b. Illegal Contents of Stored Data 23

3. Illegal Disclosure and Misuse of Data 24
a. Personal Data Covered by Traditional Secrecy Protection 24
b. Non-secret Personal Data 25

4. Infringements of Formalities of Privacy Laws 25

C. Further Abuses and Questions of Definition 26

1. Offences Against State and Political Interests 26
2. The Extension to Offences Against Personal Integrity 26
3. Resulting Questions of Definition 27

III. EXTENT, IMPACT, AND FUTURE DEVELOPMENT OF COMPUTER CRIME 29

1. Extent of Computer Crime 29
a. The Number of Known Cases — A Survey of International Computer Crime Studies 29
b. The Problem of the 'Dark Figure' 33

2. Extent of Losses 34

3. Future Developments 35

4. The Need for Further International Criminological Research 36

IV. THE LEGAL PROBLEMS OF COMPUTER CRIME 37

A. Computer-related Economic Crimes 37

1. Fraud by Computer Manipulation 38
a. Problems of Traditional Law 38
b. New Laws Enacted 42
c. Bills Planned 48
d. Comparative Analysis of Reform Projects 50
e. Suggestions for Legal Policy 51

2. Computer Espionage, Program Piracy, and Copying of Chips 52
a. Protection of General Data in Computer Systems 53
b. Additional Protection of Computer Programs 63
c. Additional Protection of Integrated Circuits 74

3. Computer Sabotage 78
a. Problems of Traditional Law 78
b. New Acts and Bills 79
c. Suggestions for Legal Policy 81

4. The Unauthorized Use of Computers 81
a. Problems of Traditional Law 81
b. New Acts and Bills 83
c. Suggestions for Legal Policy 84

5. Unauthorized Access (Protecting the Integrity of Computer Systems) 86
a. The Present Legal Situation 86
b. Reform Proposals 87
c. Evaluation and Suggestions for Legal Policy 89

6. Tax Fraud and Customs Offences 90
a. Computer-Assisted 'Traditional' Tax Fraud 90
b. Accounting Practices and Tax-evaluation with respect to Software in the National Area 91
c. Tax and Customs Problems Concerning Transborder Data Flows 91
d. Recommendations for Legal Policy 92

7. Summary: The Recommendations of the OECD Working Group 92

B. Computer-related Infringements of Privacy 94

1. The Existing International Framework 94
a. The OECD Guidelines 94
b. The Council of Europe Convention 95
c. The Resolutions and Recommendations of The European Communities 96

2. The General Concepts and Differences of National Legislations 96
a. The Present State of Legislation 96
b. Comparative Analysis 100

3. Penal Concepts and Criminal Offences of Privacy Laws 102
a. The Different Scopes of Application 103
b. The Different Acts Covered 103
c. Summary and Conclusions 108

4. Suggestions for Future Action 108

C. Procedural Problems 110

1. Evidence from Computer Records 110
a. Differences between Continental and Common-law Countries 110
b. New Acts and Bills in Common-law Countries 111
c. International Co-ordination, especially in Civil Procedural Law 113

2. Procedural Problems in International Computer-crime Cases 113

D. The Need for Comparative Law and International Co-operation 114

V. THE SECURITY MEASURES OF COMPUTER-USERS 117

A. Aims and Scope of Safety Strategies 117
1. The Aims to be Achieved 117
2. The Threats to be Covered 118

B. The Establishment of a Security Strategy 118
1. The Need for Risk-awareness and Task-force Organization 118
2. Safeguard-determination 119
a. Identification of Assets 119
b. Risk-evaluation 119
c. Safeguard-selection 120
3. Testing the System and Implementing Possible Countermeasures 121
a. Perpertrators' Organizational Countermeasures 121
b. Perpertrators' Countermeasures in the Field of Operating and Application Programming 122
c. Perpertrators' Countermeasures in the Field of System Programming 123
d. Wiretapping and other 'Technical' Methods 123
4. Implementation, Control, and Updating of the Safety System 124

C. The Main Elements of an Effective Safety System 125
1. Personal and Educational Safety Measures 125
a. Controls 125
b. Motivation, Education, and Codes of Ethics 126
2. Physical Safety Measures 126
a. Architectural Design 126
b. Building Materials and Equipment 127
3. Organizational and Technical Safety Measures 127
a. General Control Measures 128
b. Special Input Controls 130
c. Special Communications Controls 130
d. Special Processing Controls 130
e. Special Data-storage Controls 131
f. Special Output Controls 132
g. Special Protection of Licensed Programs 132
4. Internal Auditing 133
5. Insurance against Computer Crime 134
6. Formulation of Contracts 135
7. Proceedings and Legal Action in Cases of Suspicion and Loss 135

D. International Aspects 137

VI. THE PROSECUTION OF COMPUTER CRIME 139

1. Difficulties of Discovery and Detection 139
   a. Disguise of Crime 139
   b. Hidden Traces 139
   c. Non-visibility of Evidence 140
   d. Encoding of Evidence 141
   e. Erasure of Evidence 141
   f. Large Numbers of Data 142
   g. Inexperience of Prosecutors 142
   h. Legal Uncertainties and National Frontiers 142

2. Measures to be Taken 142
   a. Special Investigation Training in Various Countries 143
   b. Necessary Content of Computer-crime Investigation Courses 144

VII. SUMMARY: THE NEED FOR FURTHER RESEARCH, ACTION AND INTERNATIONAL CO-OPERATION 147

Notes 149

APPENDIX 1: INTERNATIONAL SELECT BIBLIOGRAPHY 183

A compilation of the main computer-crime studies originating from Australia, Austria, Belgium, Canada, Denmark, the Federal Republic of Germany, Finland, France, Italy, Japan, Luxembourg, the Netherlands, Norway, Spain, Sweden, Switzerland, the United Kingdom, the United States, and international organizations.

APPENDIX 2: INTERNATIONAL *CORPUS JURIS* OF COMPUTER-CRIME STATUTES 197

A compilation of computer crime acts and bills of Australia, Austria, Canada, Denmark, Finland, France, the Federal Republic of Germany, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, the Republic of China, Spain, Sweden, Switzerland, the United Kingdom and the United States.

Index 269

I.

Introduction: The Emergence of a New Threat

Western societies are currently encountering a second Industrial Revolution. This 'revolution of informatics', which is replacing the work of human minds by machines, will be more transformative than the mechanical Industrial Revolution of the nineteenth century, which replaced physical work by machines. The worldwide advances of business and personal computers, the increasing extent of storage and processing capabilities, the miniaturization of computer chips installed in industrial products, the fusing of information-processing and new information communication technologies, as well as research in the field of artificial intelligence, all illustrate the present development, often described as the turn to the 'information age'.[1]

This triumphant march of computer applications not only has an advantageous side but also leads to the crucial importance of the operation and security of computer systems for business, administration, and society. In the business community, for example, the majority of monetary transactions is administered by computers in the form of deposit money. Balance sheets are prepared with computer support. A company's entire production is frequently dependent on the functional ability of its data-processing (DP) system. Furthermore, many businesses store their most important company secrets in a computer. Modern administration relies on computer technology and databanks in a similar way. Sea, air, and space-control systems, medical supervision as well as Western defence also depend to a great extent on modern computer technology.[2]

Because of this dependency, the increasing level of criminal offences involving DP systems registered over the last decade in the United States, Western Europe, Australia, Japan, and now even in the socialist States represents a threat to individual companies as well as to a country's economy and society as a whole. This danger has been increasingly recognized in recent years and has led to national and international concern about the new threat which is called 'computer crime'.

According to a definition worked out by a group of experts invited by the

OECD to Paris in May 1983,[3] the term *computer crime* (or 'computer-related crime') is defined as any illegal, unethical, or unauthorized behaviour involving automatic data-processing and/or transmission of data. The breadth of this definition is advantageous, as it permits the use of the same working hypothesis for all kinds of criminological, criminalistic, economic, preventive, or legal studies. Obviously, this does not prevent each of these studies from dealing only with the phenomena of computer crime, which cause computer-specific problems in its own discipline.[4]

Using the broad definition of the OECD as a working hypothesis,[5] this book will provide an international survey of the main problems surrounding the new phenomena. In the proceeding chapter the various forms of computer crime are described. The third chapter covers the extent, impact, and future development of computer offences. In the three chapters following this phenomenological analysis, the manner in which the legislature, business community, and law-enforcement agencies have so far dealt with these problems are discussed, as well as those measures which ought to be taken in the future. Finally, a summary stresses the need for further action and international co-operation.

II.

The Phenomena of Computer Crime

Up to the present three main groups of computer crime (falling within the OECD definition) have been revealed: computer-related *economic crimes* such as computer fraud, computer espionage, and computer sabotage; computer-related *offences against personal rights*, especially against the citizens' right to privacy; and computer-related *offences against superindividual interests* such as offences against national security, control of transborder data flow, integrity of computer-based procedures and data-communication networks, or democratic legitimation of computer-based parliamentary decisions.

The following analysis of these phenomena is arranged according to the actual frequency and importance of the respective acts. It first describes the various computer-related *economic crimes* (*infra*, A). Then it investigates the group of computer-related *infringements of privacy* (*infra*, B). Finally the remaining *other phenomena* and definitional questions are discussed (*infra*, C).

A. COMPUTER-RELATED ECONOMIC CRIMES

Computer-related economic crimes constitute the main field of computer crime today. Excluding accidental and negligent damage to computer systems, six main categories of computer-related economic crimes have been developed. These are

(1) Fraud by computer manipulations against DP systems;
(2) Computer espionage and software theft;
(3) Computer sabotage;
(4) Theft of services;
(5) Unauthorized access to DP systems; and
(6) Traditional business offences assisted by DP.[1]

1. Fraud by Computer Manipulation

Fraud against DP systems by computer manipulation involves the changing of data or information for purposes of financial gain. The following analysis describes the objects, the methods used, and the perpetrators of this new type of fraud.

a. OBJECTS OF COMPUTER-RELATED FRAUD

The objects of computer-related fraud are *data representing assets* in DP systems. In the majority of computer fraud cases the assets represented by computer data are *intangible objects* such as deposit money, claims, working time, credit ratings, and results of calculations of balances. Cases known at present are primarily manipulations concerning salaries, invoices, pensions, and social security payments as well as manipulations of the account balances of bank computers. Because of the increasing replacement of cash money by deposit money, this field of computer crime will also be the main area of computer fraud in the future. In Europe the trend towards a cashless society is especially illustrated by the widespread system of money transfer orders and giro services, which became the main payment systems in both the private and the business sectors. In the United States the replacement of cash money and paper-based payment systems with 'electronic blips' is especially shown by point-of-sale (POS) and other electronic funds transfer systems (EFTS), in which payments are made by inserting a plastic card into a terminal connected to a computer. All over the world, EFTS are common in the banking area. The four major funds transfer systems in the United States—Fedwire, Bankwire, CHIPS, and SWIFT, for example—transmit about $300 billion per day domestically and $600 billion per day internationally.[2]

> It is obvious that these developments in the economic and technical areas attract criminals for special reasons. Because the sums transferred or processed by computer systems are very high and because electronic money can be 'created' by the perpetrator, the amounts of losses in these cases are generally very high. The widely reported case of Mark Rifkin is an example. In 1978 he fraudulently managed to get $10.2 million transferred from the Security Pacific National Bank in Los Angeles to a New York bank account by means of a telephone call.[3]

In some cases the data being the object of computer fraud represent *tangible and corporeal objects* which are taken away by the perpetrator after the manipulation of the computer system. This concerns especially cash money, materials, merchandise, or goods. Manipulations concerning these classic objects of crime generally result in smaller losses than manipulations of intangibles, since the losses here are limited by the actual amount of goods available.

Two West German cases which were reported to the police in 1984 and 1985 can be singled out as examples of fraud concerning such classic objects of inventory. In the 1984 case a programmer and a stock clerk had altered the program and the databases of a spare-parts store's computer so that spare parts taken away by them were invoiced at very low prices. The losses in this case amounted to DM 31 000.[4] In a similar case in 1985, which also concerned the manipulation of spare parts, the perpetrators embezzled merchandise valued at about DM 300 000.[5]

A *specific group* of computer crime cases primarily concerning tangible cash money, goods, and services registered by computer systems has now been made possible by the increasing number of *cash dispensers* installed by banks and by *electronic high-efficiency vending machines* equipped with electronic sensors.

In Japan the installation of *cash dispensers* (CD machines) and automatic teller machines (ATMs) is the most advanced in the Western world. By 1981 23 627 CD machines had been installed and 66 450 CD cards were in use. As a result the manipulation of cash dispensers represents one of the main problems of computer crime. In 1981, 288 cases of CD crime were known to the police, 83.3% of which involved the use of stolen cards, 9.7% the use of forged cards, 4.9% cards received by fraud or blackmail, and 2.1% lost-and-found cards. The number of cases reported to the police increased to 472 in 1982 and to 642 in 1983.[6] In the United States the US Bureau of Statistics estimated that in 1983 banks suffered losses of about $70–100 million by the illegal use of CD cards. (For the manipulation techniques used in these cases, see *infra*, b, pp. 9 *et seq.*)

A similar development is now taking place in the field of *electronic high-efficiency vending machines*. Here, too, in Japan the technical development of these machines is the most advanced in Western countries. At the end of 1982 in Japan there were about 4 900 000 automatic vending machines, 200 000 of which were high-efficiency machines which could read and identify banknotes. The first manipulation of these systems was reported to the police on 30 July 1982 at Osaka. From this date until December 1982, 328 cases in 37 prefectures were reported, of which 181 concerned vending machines; 98, money-changing machines; 43, amusement machines; four, pin-ball machines; and two, automatic ticket machines. At the end of 1982, 39 of these cases were cleared and 58 people were arrested, of whom 23 were members of organized crime groups.[7]

An analysis of the *differences between traditional fraud and computer fraud* in the field of the objects of the crime shows that the assets now represented and manipulated in DP systems were the target of traditional fraud long before the computer existed. This is also true in the field of intangible assets, because the change from tangible to representative or symbolic assets in countries' economies started centuries ago. However, what is new about the object of computer manipulations is the fact that the information representing these assets is no longer stored on paper, in a visible, easily readable form but in an invisible and machine-readable concentrated form in electronic storage devices. This *change from paper-represented assets to paperless-represented* *assets* is, as will be shown later, the reason for problems both in the scope and the detection of crime and in the application of existing legislation. Concerning the object of the crime, computer-related and traditional property crimes differ not only in this qualitative aspect but also quantitatively. This *quantitative difference*, which is caused by the *high values handled in DP systems*, will be dealt with later in connection with amounts of losses in computer crime.[8]

b. MODI OPERANDI: THE METHODS OF MANIPULATION

As the information stored in DP systems is no longer handled by humans but by computers, the offender now has to proceed differently in order to achieve his aim of changing information. It is therefore the *mode of perpetration* which forms the *main difference between traditional fraud and computer fraud.*

For a better understanding of the various *methods of manipulating DP results* the computer has to be regarded as a DP system, i.e. as a system into which the data to be processed and the required type of processing are fed (via the program and additional console inputs) and which automatically outputs the result of this processing. The offender can either feed the computer incorrect data from the beginning (input manipulations), interfere with the correct processing of the computer (program, console, and hardware manipulations), or subsequently falsify the initially correct result given by the computer (output manipulations). In computer systems using data communication, especially remote DP, additional manipulations in the field of data transfer are possible. Special methods of manipulation also exist in the field of cash dispensers. All these manipulation techniques have been successfully applied in practice.

Input manipulations make up the majority of computer manipulations discovered up to now. These can be carried out mainly by the adding, omitting, changing, exchanging, or incorrect posting of input. Such 'data-diddling' is primarily committed by clerks, data typists, transaction participants, and operators responsible for the collection, checking, transmission, and input of data to be processed.

> As an example of an input manipulation committed by a clerk, the case of a savings bank in South Germany can be cited. The female perpetrator, who was working as a teller in a local branch of the bank, in February 1983 transferred DM 1.3 million to her friend's account early in the morning by simply inputting the respective credit into her terminal. The bank's well-developed control and safety system would have detected this manipulation no later than noon. However, the online transmission of the credit by remote DP and the speed of a modern computer system made it possible for the teller's friend to withdraw three cheques totalling DM 1.28 million some minutes later at another branch of the bank.[9]
>
> Another example of a typical input manipulation is the case of a DP employee in Zurich who succeeded in manipulating the automatic foreign payments transac-

tions of one of the biggest Swiss banks. The employee, who was working as an operator and data-checker for the bank, intercepted various transfer orders from his accomplices in the encoding department of the bank and then, instead of feeding the computer the correct transfer amounts, fed a thousand times the amount each time. He cleverly avoided the security measures set up by the bank in order to prevent such manipulations. Thus, when DM 98 were, for example, deposited in Frankfurt, his accomplices, drawing the money in Lugano and Davos, did not receive 100 Swiss francs but 100 000 Swiss francs. Similarly, for their $97 deposited in New York, they did not receive 251 but 251 000 Swiss francs. The perpetrators made a profit of about 700 000 Swiss francs through these manipulations. They were sentenced to prison and put on probation in 1976.[19]

Compared with input manipulations, which in many cases can be carried out without any knowledge of DP, the *modus operandi* of *program manipulations* is more computer-specific and, above all, much more difficult to discover. These manipulations are committed either by *changing the company's existing programs* (especially by adding 'Trojan-horse' routines or using special versions of the 'virus-programs', described below) or by *applying additional programs*, written by the perpetrators. These additional programs can either be self-written or standard utility programs which are powerful tools for emergency situations and able to bypass most security measures (for example the widespread 'superzap' utility).[11] The following examples show that the offender can use such program manipulations to bypass security checks and tuned circuits set up for the prevention of computer offences and that he can disguise his crime almost perfectly.

The offender was employed as a programmer at a large West German corporation. Using a program especially written for the purpose, he entered the information on the salaries of fictitious people into the data memories containing company salary information and inputted his own account as the account to which the fictitious salaries should be transferred. This salary manipulation, which was successfully carried out even in this simple form at several West German companies,[12] would have been discovered in the company concerned as the computer prepared wage-slips, checklists, account summaries, and balance sheets which were carefully checked and evaluated by the company. In order to prevent discovery by these control printouts the offender first made changes in the salary payments program to ensure that no pay-slips were printed for payments to the fictitious employees and that the payments did not appear in the checklists produced by the computer. By further manipulation of the program which produced the company's accounting summaries and balance sheets the perpetrator finally succeeded in having the embezzled amounts deducted from the income tax to be paid to the tax office. Thus the sums did not appear as deficient amounts in the company's accounting summaries and balance sheet. The offender fraudulently made DM 193 000 before the manipulation was discovered by chance. In 1978 he was sentenced to two years' imprisonment for fraud and breach of trust.[13]