Telecommunications Fraud
Organized approaches to fight it

Presentation for
FIRST Technical Colloquium
February 7. 2000
By Security Supervisor
Keld Frimann Nielsen Tele Denmark

Agenda
- Telecommunications approach to security
- Fraud types and examples on fraud
- Amount and trends on fraud, worldwide
- Methods and tools to combat fraud
- International cooperation
- Presentation on CFCA (Communication Fraud Control Association)
- Tele Denmark activities on fraud prevention and detection
- Questions?
Telecommunications approach to security

Security Statements (1.)

- Security is a competitive parameter in the liberalized telecommunication world.
- Security protects the customers against incorrect bills and misuse from third parties.
- Security protects the company against accidental or by conscious caused losses or misuse of the telecommunication network.
Security Statements (2.)

- Security protects the employees against unjustified accuse on participation in criminal activities.
- Security is a part of the company image and a trade mark on all telecommunication products.
- Security is a demand from the community.

What are we to protect us against? (1.)

- Customer complains on product quality.
- Impenetrable or incorrect billing.
- Unauthorized physical access to the customers telephone line. (clip-on fraud)
- Unauthorized logical access to the customers telecommunication network and services.
- Unauthorized physical access to exchanges, infrastructure and buildings.
What are we to protect us against? (2.)

- Unauthorized logical access to network, exchanges and control systems.
- Unauthorized access to the administrative EDP systems and databases.

Who are we to protect us against? (1.)

- Criminals who wants to make phone calls free of charge.
- Organized criminals who bases there business on resell of stolen telecommunication products.
- Criminals who wants to disturb or destroy the telecommunication infrastructure.
Who are we to protect us against? (2.)

- International operating criminals who wants to cover there activities by looping into the global telecommunication network.
- Persons with legal access to network, EDP systems or buildings but
  - consciously or unconsciously becomes a victim to criminal elements.
  - permit some act of revenge against the company
  - have been mentally ill or unbalanced.

Fraud types and examples on fraud
Physical access, (Clip on)

The access network

Clip on: Illegal parallel connection on the subscriber line and make someone else pay for the calls

Customers Private Equipment Fraud

CPE Fraud: Stressing and/or misuse of a customer's PABX to get new dialing tone and make free calls
Classic Fraud types

- Subscription Fraud: Misuse of the operators credit on payment of the bill
- Mobile Fraud: Cloning of analog mobile phones
  - Theft of SIM cards and handsets
  - Roaming Fraud, (misuse of the lack in timing for exchange of billing information)
- Carding Fraud: Misuse of stolen, hacked or shoulder-surfed card numbers and private PINS
- Boxing Fraud: Illegal stressing of national or international channel associated signaling systems

Fraud types

- Payphone Fraud: Physical or logical manipulation on payphones to get free calls

Example: Eternity cards
Telephone card modified with eternity chip.

The chip is covered with tape.

Fraud types

- Social engineering: Structured misuse of naive peoples to get confidential information or to sell fictive items (winnings, pyramid games etc.)
- Premium rate service Fraud: Misuse of others phones to generate calls to 900 services or specific countries to obtain profit from the service provider
Amount and trends on Fraud worldwide

Estimated Fraud losses

- Annual Fraud losses U.S. 1997 - 1998
  - Mobile Fraud $650 Million
  - All telecommunications $9 Billion
    (United States Secret Service)
- Annual Fraud losses Europe 1998
  - Euro 1 Billion
    (FIINA conference)
- Personal estimate Europe: Euro 2-3 Billion
- Worldwide all telecommunications 1999
  - $20 Billion
    (Nordtel, CFCA and others)
Trends on Fraud

- Fraud is increasing
- Internet provides numerous recipes on how
- Fraud is becoming more and more sophisticated
- Fraud does not respect boarders and involves often more operators network
- The increase in integrated services “invites” criminals to look for “security holes”
- Interconnect points for different networks are obvious points for attacks

Methods and tools to combat Fraud
How do we combat Fraud?

- Security policy for all units within the company
- Continuously education of security staff
- Awareness campaign for all employees
- Security inspection on new products
- Registration of all abnormal incidents
- “Listen” to customers complains
- Cooperation with the authorities (police etc.)
- Cooperation with other operators
- Supervision of the network
- Fraud Management Systems

Tools (Fraud Management Systems)

- Real time supervision based on “Common channel signaling system no 7.” (all calls)
- Creation of traffic patterns
- Setting up thresholds for alerts
- Automatic alert on suspected traffic, behavior or other abnormal changes
- Integration of information from different systems, (customer database, billing database, traffic database)
- Manual investigation on alerts
International cooperation

**International associations handling telecommunications Fraud**

- **ETNO**: European Telecommunications Network Operators (Standardization)
- **FIINA**: Forum for International Irregular Network Access (Operational, incidents, methods)
- **CFCA**: Communications Fraud Control Association (Educational exchange of experiences, Fraud alerts)
- **Nordtel, NS/T**: Nordic security group, (exchange of experiences and incidents)
Presentation on CFCA  
(Communications Fraud Control Association)

CFCA - Goal

- Founded in 1985, CFCA is a not-for-profit international educational association working to help combat telecommunications fraud. CFCA seeks to promote a close association among telecom security personnel, to enhance their professional status and efficiency, and to serve as a clearinghouse of information pertaining to the fraudulent use of telecommunications services.
Membership

- Interexchange Carriers (IXC), Local Exchange Carriers (LEC), CLECs and ILECS, Private Network Companies, Law Enforcement, Officers & Agents, CPE-PBX users, E-mail providers, Security Product Vendors, Corporations that use telecommunication services (i.e. banks, universities, department stores, etc.)
- Number of members app. 240

CFCA - Objectives

- Educational conferences
- Education CCSP (Certified Communications Security Professional)
- Weekly Fraud Alert
- Expert forum (Questions from members)
- Communicator (Quarterly journal on Fraud issues)
- Fraud handbook
- Awareness brochures on Fraud
- Membership directory
CFCA - planned program 2000

- 2000 International Spring Conference
  “Fraud in the 21st Century”
  2 - 5 May Edinburgh Scotland

- Fifteenth Annual Meeting and Conference
  and Seventh Annual Exhibition
  20 - 23 June Washington DC USA

- 2000 Fall Conference
  4 - 6 October Phoenix Arizona USA

WWW.CFCA.org  FRAUD@CFCA.org

Tele Denmark activities on Fraud prevention and detection
Organizational and Collaboration Structure

President & CEO Henning Dyremose
Responsible for overall Security

Net & Installation
Ruth Pierson

Finance, CFO
Hans Munk Nielsen

Operational Security Units – Professional reference

Domestic Security Group

Primary Focus: External/ Customer

Jørgen Bo Madsen

PA Security

Customer Security

Network Security

Cable TV Security

Physical Security

Auditing

Ad hoc Group

Primary Focus: Internal /Legislated

Per C. Andersen

Ad hoc Group

Ruth Pierson

Organizational and Collaboration Structure

Approaches

- Corporate security policy
- Dedicated security policies for all units
- Security inspection program for new functions
- Security program for the access network
- Security program for access to buildings
- Security program for the IT network
- Supervision program for traffic etc.
- Investigation on suspicion
- Cooperation nationally and internationally
- Cooperation with the police
- Plan to implement a Fraud Management System this year
Questions?