CPNI Training

November 27, 2018

Roxi Hacker
Interstate Telcom Consulting, Inc.

C P N I

Customer Proprietary Network Information

History

- **Telecommunications Act of 1996**
  - In 1999 – FCC implementation
  - In 2007 – new compliance rules
  - In 2009 – violations
  - In 2017 – reinstatement
- **47 C.F.R.**
  - § 222
  - § 64.2003-64.2011

C P N I

Customer Proprietary Network Information

- "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship"
- "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier"

47 C.F.R. §222

- **Privacy of customer information**
  - Every telecommunications carrier has a duty to protect the confidentiality of proprietary information belonging to customers
- **Confidentiality of carrier information**
  - A carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use that information only for such purpose, and shall not use that information for its own marketing efforts

What is considered CPNI?

- **Examples of CPNI**
  - *Call Detail CPNI*
    - Phone numbers called and calling patterns (toll or local)
    - Time, date, duration of calls
  - *Non-Call Detail CPNI*
    - Customer's remaining minutes of use
    - Amount customer spends on services on a monthly basis
    - Optional services used (call waiting, call forwarding, etc.)
    - Sensitive personal information
    - For business customers – number of lines

What is NOT CPNI?

- Customer Name
- Address
- Telephone Number
- Public Information
- Non-Regulated Services

Who Must Comply?

- **Telecommunications Carrier**
  - *POTS*
  - *CMRS*
  - *VoIP*
  - *SIP Trunk*

47 C.F.R. §222

- **Confidentiality of CPNI**
  - Disclosure request by customer
  - Aggregate customer information

Obligation To Protect CPNI

- Prevent access of CPNI by pretexters and data brokers
- Can only provide CPNI to the customer of record
- Carrier use of CPNI for marketing
- FCC fines if CPNI is not protected or if a carrier does not have procedures in place to protect CPNI

CNPI Use

- **When can you use CPNI?**
  - Required by law
  - With customer's approval
  - To provide the service

Customer Authentication

- Verify customers by password / PIN
- Notice sent to address of record of account changes
- Forgotten password / security question
- Identification
- Individual(s) listed on account
- On-line payments / service

Customer Notification of Account Changes

- **Carriers are required to notify customers immediately if the following are created or changed:**
  - A password
  - A back-up for forgotten passwords
  - An online account
  - The address of record
- **The customer notification may be through a voice mail to the telephone number of record or by mail to the address of record**
- **The notification must not disclose what account information was changed**

Online Account Access

- **Must be password protected**
- **Carrier may determine the password length and format**
- **Carriers do not have to reinitialize existing passwords**
- **Can create a back-up question for forgotten passwords**
- **May not relay on readily available biographical information** (social security number, mother's maiden name, address, date of birth, etc.) **or account information to authenticate a customer's identity**
- **Carriers are expected to block access to a customer's account after repeated unsuccessful attempts to log into that account – but it is not mandatory**

Business Accounts

- The FCC does not require carriers to apply the same authentication rules to business customers that are served by a dedicated account representative and that there is a contract that covers the carrier's protection of CPNI
- We recommend that you apply the CPNI rules to both business and residential customers alike

47 C.F.R. §64.2007

- **CPNI approval**
  - Opt-In
    - *Valid until customer requests Opt-Out*
    - *Oral, written or electronic*
  - Opt-Out
    - *Every two years*
    - *Written or electronic – NOT oral (except one-time use)*
    - *30-day waiting period*
  - One Time Use
    - *Oral*

47 C.F.R. §64.2008

- **Customer notification**
  - Annual Notification
    - *Customer's rights*
    - *Customer's responsibility*
  - Opt-Out
    - *Every two years*

47 C.F.R. §64.2009 and §64.2010

- **Safeguards**
  - Train employees about using CPNI and have express disciplinary process
  - Must obtain supervisory review and approval of all marketing campaigns that use CPNI
  - Must maintain a record of the marketing campaigns listing the following information
    - *Description of campaign and companies involved*
    - *Description of CPNI used*
    - *Date and purpose of the campaign*
    - *Products or services offered*
    - *Maintain record for one year*
  - Must have a system in place to keep track of customers status (approve/not approve)

Training

- **Employees should be trained**
  - Time of hire
  - Suggested annually
- **Disciplinary process**
- **Supervisory process**
  - Review and approve marketing campaigns using CPNI
  - Annual compliance certification – March 1st

Record Keeping

- **CPNI status – readily available**
- **Marketing campaigns – supervisor approval**
  - 1 year
- **Proof of training**
- **Opt-Out**
  - 2 years
- **Compliance / certification**
- **Documentation**

47 C.F.R. §64.2011

- **Notify law enforcement within 7 business days of any unauthorized disclosure**
- **Notify customers within 7 business days after notifying law enforcement**
- **$150,000 / violation or each day of a continuing violation**
  - $1.5 million maximum
- **Annual certification – March 1st**

Annual Certification

- **January 1st – March 1st**
  - FCC Electronic Comment Filing System (ECFS) 06-36
  - On-line website http://apps.fcc.gov/eb/CPNI

CPNI vs. Red Flag Rules

- **CPNI – protection of telecommunications customers from pretexting and unauthorized use or disclosure of personally identifiable customer information**
- **Pretexting – using identity of another person to gain access to call detail or other personally identifiable customer information**
- **Red Flag Rules – protect all customers with covered accounts from theft of their identity and to protect the company and customers from all forms of identity theft**
- **Identity Theft – fraud committed or attempted using the identifying information of another person with authority**

Identity Theft Order

- In December of 2007, the Federal Trade Commission (FTC) and five federal bank regulatory agencies (FDIC, OCC, Federal Reserve, OTS, and NCUA) jointly issued the final rules and guidelines implementing Section 114 of the Fair and Accurate Credit Transactions Act (FACT Act)

- Under these regulations, the "Red Flag Rule" was adopted which requires the development, implementation, and maintenance of an Identity Theft Prevention Program

Identity Theft Order

- **Creditor**
  - Any entity which regularly extends, renews, or continues credit
  - Any entity who regularly arranges for the extension, renewal or continuation of credit
  - Any entity that participates in the decision to extend, renew, or continue credit

Identity Theft Order

AND …

- **Regularly and in ordinary course of business:**
  - Obtains or uses consumer reports directly or indirectly in connection with a credit transaction
  - Furnishes information to consumer reporting agencies in connection with a credit transaction
  - Advances funds to or on behalf of a person based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person…

    EXCEPT *for advancement of funds for "expenses incidental to a service provided by the creditor to that person"*

Identity Theft Order

Or …

- **Is any other type of Section 702 Creditor* that the agency determines is appropriate by regulation because it offers to maintain accounts that are subject to a "reasonably foreseeable risk" of identity theft**

**Section 702 of Equal Credit Opportunity Act*

Program Review

- **Program must be written and include procedures to:**
  - Identify relevant red flags
  - Detect red flags
  - Respond to red flag detection
- **Program must also be updated periodically to address changing risks**

Program Review

- **Administration of the program**
  - Approval by the board or committee
  - Senior management oversight of the program
  - Train staff
  - Oversee service provider arrangements

Red Flags

- **Four categories of identity theft**
  - Financial ID Theft
  - Business / Commercial ID Theft
  - Criminal ID Theft
  - Identity Cloning
- **Theft of personal information can occur in a variety of ways**

Red Flags

- **Stolen identities can be used for many different fraudulent purposes**
  - Open new wireline or wireless services
  - Obtain cable TV or video service
  - Apply for jobs
  - Write bad checks
  - Clone ATM cards / calling cards
  - Obtain utility service
  - Obtain government benefits

Red Flags

- **Sources of Red Flags**
  - Alerts or Notifications from Consumer Reporting Agency
  - Suspicious documents
  - Suspicious personal information
  - Unusual use of covered account
  - Notice directly from customers or law enforcement

Detection of Red Flags

- **Establishing a new account**
- **Changing an existing account**
- **Bring matter to company appointed Red Flag Coordinator**

Responses to Red Flags

- Watch list
- Contact affected customer
- Change passwords, PINs, security codes
- Close covered account
- Re-open under new account number
- Notify law enforcement
- Determine no response is necessary

Responses to Red Flags

- **To determine the appropriate response**
  - Security breach
  - Notice from customer
  - Notice from other entity

Red Flag Rule - Training

- **Employee should be trained upon hire**
  - Suggested annually – best practice
- **Program available written or electronically to employees**
- **Whenever changes are made to program**

Red Flag Rule - Compliance

- Board minutes containing approval of Identity Theft Manual
- Board minutes containing annual review compliance
- Board minutes when Red Flag detection is discussed
- Complete detection / response sheet for tracking

Red Flag Rule - Penalties

- **A covered entity that fails to comply with the Red Flag Rules may be subject to civil monetary penalties**

- **Civil monetary penalties for noncompliance are based on the Consumer Price Index and stand at $3,500 per violation** (repeated violations after an order to comply, the FTC can file suit)

?

130 Birch Avenue West
P.O. Box 668
Hector, MN 55342

E-mail: roxi@interstatetelcom.com
Phone: 320-848-6641
Fax: 320-848-2466

www.interstatetelcom.com