Sprint Nextel

Sprint

Together with NEXTEL

What You Need To Know About Customer Privacy and CPNI

Training for All Sprint Non-Employees

Non- Employees

ATTENTION / PLEASE NOTE:

You are not an employee of Sprint Nextel.

You are an employee of a Vendor/Contractor who provides services to Sprint Nextel.

As such, it is important that you complete this privacy training so that you better understand the privacy-related laws and Sprint Nextel's privacy policies.

You must comply with all Sprint Nextel privacy policies and procedures and all applicable privacy laws.

The Importance of Customer Privacy

- The Law
  - The FCC's Customer Proprietary Network Information (CPNI) rules
  - Other Federal and State laws and regulations regarding the collection, storage, access, use or disclosure of personal information
- Customers' increasing focus on privacy rights
- Failure to Comply
  - Potential disciplinary action up to and including termination
  - Fines and criminal prosecution

Customer Information

As a part of your job, you may have access to sensitive customer information.

Examples include:

- SSN
- Contact information (name, address, telephone numbers)
- CPNI (rate plan, usage details)
- Billing information (credit card information)

All of this information is sensitive, but Sprint has special obligations regarding CPNI.

What is CPNI?

CPNI stands for **C**ustomer **P**roprietary **N**etwork **I**nformation

- CPNI is information about the customer's purchase and use of telecommunications services that the company obtains solely through providing those services to the customer.

- FCC's CPNI regulations govern precisely how carriers may access, use or disclose CPNI.

Categories of CPNI

- Categories of CPNI include:
  - Where, when, and to whom a customer places a call
  - When and from whom a customer receives a call
  - What types of, and how much, telecom service the customer buys
  - Location Information
  - How much the customer uses these services
  - How much the customer is billed for service

- Examples of CPNI:
  - Call Detail Records
  - Minutes of Use
  - Most information on customer invoices
  - Your location when you make a call

Why does the FCC limit use of CPNI?

- To protect customer privacy
- To promote competition among telecom carriers

Question 1

Allison is a Sprint Nextel customer. Which of the following information contained in her account is not considered CPNI?

a) Allison called (703) 555-7654 seven times last month.

b) Allison has two wireless handsets and two accounts under her name.

c) Allison's customer address is 1200 Main Street, McLean, Va.

Pick your answer and proceed to the next slide

Question 1 - Answers

a) Wrong: CPNI includes things like a customer's call-detail. The fact that Sally dialed a certain number several times would be CPNI.

b) Wrong: CPNI includes things the number of handsets on an account.

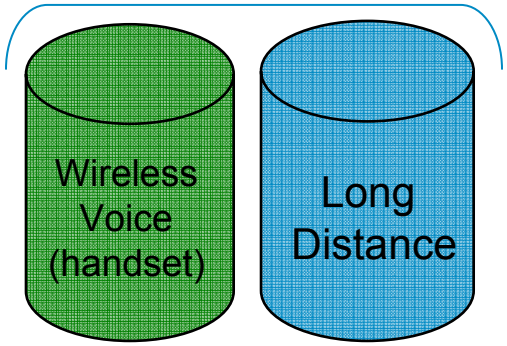
c) Right: Name and address is not CPNI. Remember, some personal information is not CPNI, but its still sensitive information covered by other laws and Sprint's privacy policy.

Please review the answers and then proceed.

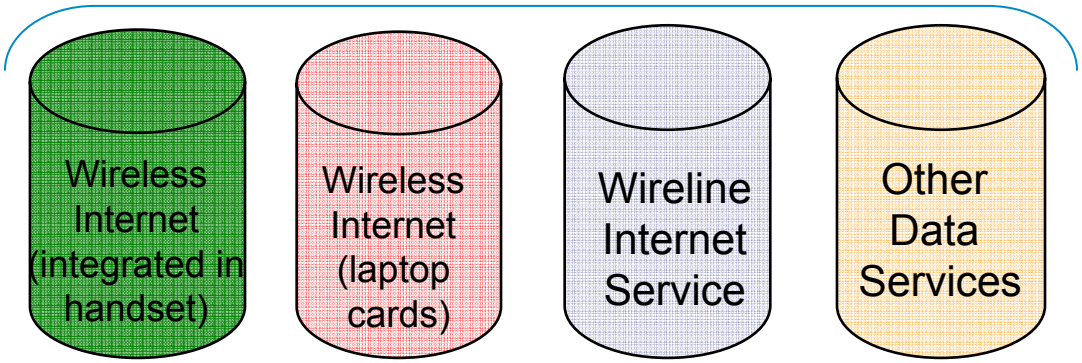
Sprint Nextel's Products and Services

- Sprint offers many different products and services that fit into 6 categories.
- CPNI applies only to telecommunication services (e.g. Wireless Voice or Long Distance) and not to Information Services.

Telecommunications Services (CPNI)



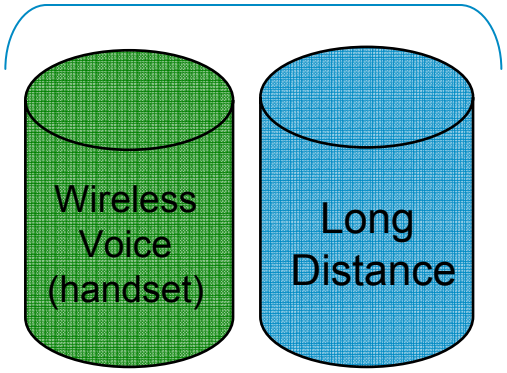
Information Services (no CPNI)



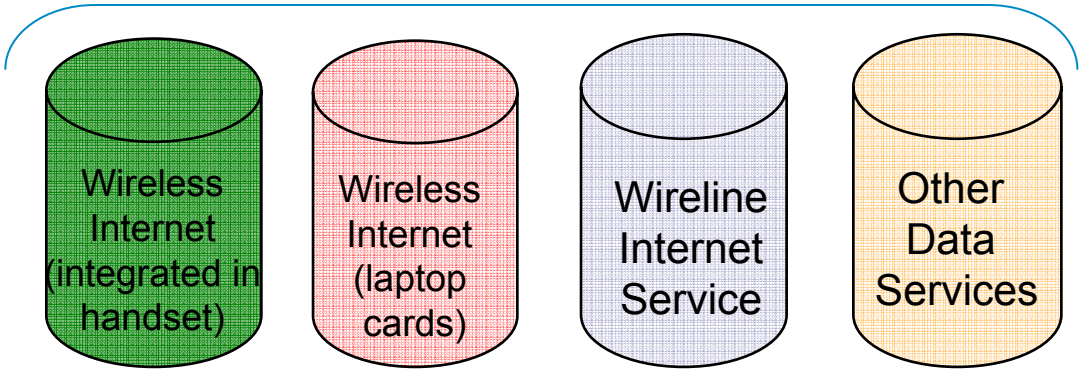
Total Service Relationship

The specific categories of telecommunications services to which a customer subscribes is called their **Total Service Relationship (TSR).**

Telecommunications Services (CPNI)



Information Services (no CPNI)

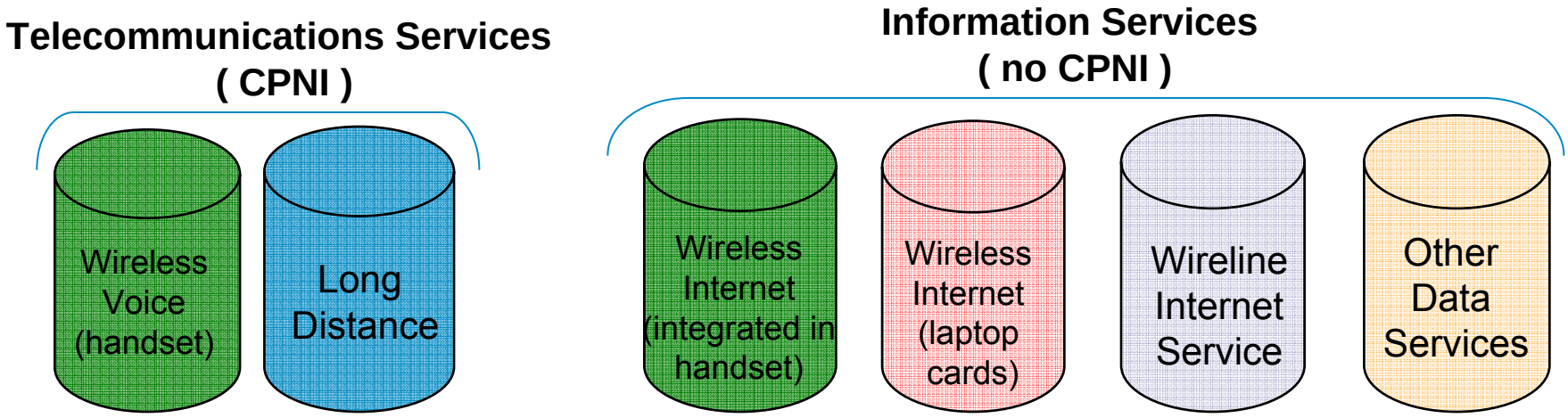


Total Service Relationship

• If a customer subscribes to more than one category of service, the customer's TSR includes all of the relevant categories.

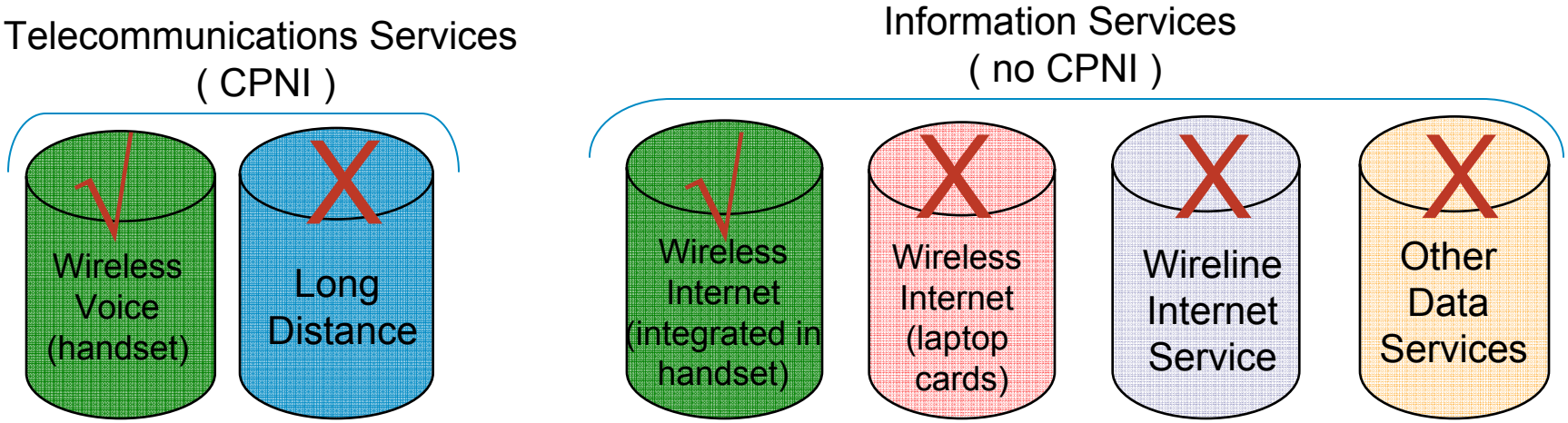
• For the CPNI related products and services, you may use CPNI to up sell more products and services that are in the same category of telecommunications services.

> The only exception to this rule is that you may use Wireless Voice CPNI to market Wireless Internet because the 2 services are integrated in the handset.



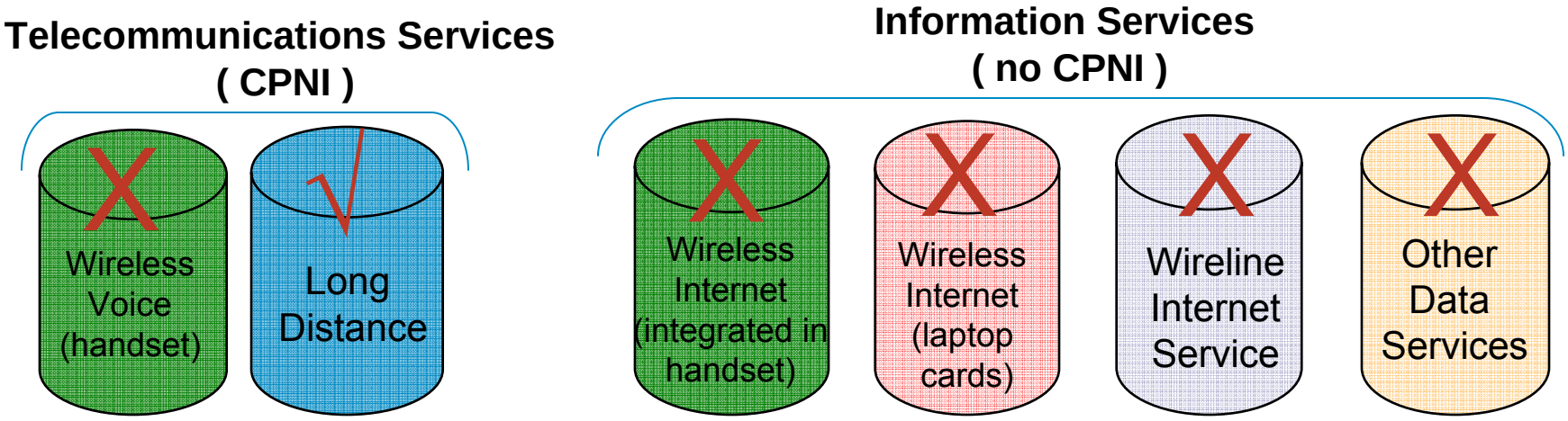
TSR: Example One

- A customer subscribes only to Wireless Voice.
- So, Sprint may use the CPNI from the Wireless Voice to market related Wireless Voice products and services. And, because in this unique case Wireless Internet is integrated into the handset, Sprint may use the wireless voice CPNI to market wireless Internet (on the handset) as well.
- Sprint may still cross sell the other products and services, but Sprint can't use the Wireless Voice CPNI to do it.



TSR: Example Two

- A customer subscribes only to Long Distance.
- So, Sprint may use the CPNI from Long Distance to market related Long Distance products and services. Sprint may not use LD CPNI to cross sell to any other products or services without customer consent.
- Sprint may still cross sell the other products and services, but Sprint can't use the LD CPNI to do it.



Question 2

Acme Company buys Sprint wireless services from your company. The CPNI rules allow you to engage in which of the following upsell activities?

a) Use information about Acme's volume of monthly wireless calls to cross sell other kinds of Sprint services (e.g. long distance service) to Acme.

b) Use information about the Sprint wireless services purchased by Acme to suggest more Sprint wireless products or services.

c) Use information about Acme's Sprint wireless services to market other products that your company offers.

Pick your answer and proceed to the next slide

Question 2 – Answers

a) Wrong. You may not use Sprint customer information to cross sell other kinds of Sprint products or services. You may use CPNI and other customer information to up sell more of the same kind of products and services. For example, you may use a Sprint wireless customer's information to up sell more Sprint wireless products or services.

b) Right. You may use CPNI derived from the customer's Sprint wireless service to market more Sprint wireless products or services to the customer.

c) Wrong. You may not use CPNI (or other Sprint customer information) to market non-Sprint products and services.

Please review the answers and then proceed.

When Can I Access a Customer's Account?

- **Providing Customer Service**: You may access the customer's account to provide customer service.

- **Up selling Sprint**: You can access a Sprint customer's account (including the customer's CPNI) to offer more Sprint products and service in the same category. You may **not** access the account to offer non-Sprint products and services or Sprint products and services in a different category.

- **Responding to emergencies and government requests for information**: Very specific rules apply to this scenario. Ask your supervisor to contact Sprint Nextel Corporate Security for instructions.

When Can I Use CPNI Without Customer Consent?

- You can access and use CPNI to sell more products and services within the categories of service to which the customer currently subscribes (i.e. the Total Service Relationship)

- Responding to emergencies and government requests for information: Ask your supervisor to contact Sprint Nextel Corporate Security.

Using CPNI: Winback & Retention

- Winback marketing: To win back customers who have already left Sprint Nextel, you may use their CPNI to market the same categories of service that they had with Sprint Nextel.

- Retention marketing: You can't use CPNI that identifies customers who are leaving for another carrier (e.g., those who have called our competitors' 800#s or for whom Sprint has received a port-out request). But you may use CPNI to identify customers who you believe may leave because of factors like decreasing levels of usage.

Question 3

John Smith was a Sprint wireless customer. John ported his telephone number to a different wireless carrier. You would like to look at John's Sprint account, including his CPNI, to offer him an incentive to return to Sprint as a customer. Select the answer that correctly indicates how you may act:

a) You may access John's account to target him for a direct mail offer about Sprint wireless services because he once subscribed to Sprint wireless services.

b) You may access John's account to target him for a direct mail offer about another carrier's wireless services because he once subscribed to Sprint wireless services.

c) You may access John's account to target him for a direct mail offer about other products and services because he once subscribed to Sprint wireless services.

d) All of the above are correct.

Pick your answer and proceed to the next slide

Question 3 – Answers

a) Correct. You may access John's Sprint account information to offer John an offer to return to Sprint wireless.

b) Wrong. You may not access John's Sprint account information to make John an offer to return to your store to purchase another carrier's wireless products or services.

c) Wrong. You may not access John's Sprint account information to make John an offer to return to your store to purchase other (non-Sprint) products or services.

d) Wrong. See answers to b) and c) above.

Please review the answers and then proceed.

Location Information

Location information is very sensitive information.

In most cases, Sprint must obtain consent from the customer or end user of a handset before we can access, use or disclose location information.

If you wish to access, use or disclose location information, **you must** contact the Office of Privacy (officeofprivacy@sprint.com) to ensure that your plans comply with the law and our policies.

Sprint's Do Not Contact Policy & Compliance Instructions

Sprint's Do Not Contact Policy addresses how Sprint honors individuals' contact preferences when conducting any of the following direct marketing activities:

- Calling/Telemarketing
- Emailing
- Direct Mailing
- Faxing (Prohibited)
- SMS/Text Messaging

The Compliance Instructions outline direct marketing compliance procedures. It explains how you may contact current, former or potential customers while honoring any do-not-contact requests that have been registered on the federal, state or internal Sprint Nextel do-not-contact lists.

You must regularly review the applicable Sprint Do Not Contact Policy & Instructions. Check with your Sprint manager for details regarding Sprint's most current policies and instructions.

Honoring Do Not Contact Preferences

Do not contact = honoring contact preferences.

You must promptly process all “do not contact” requests.

This means that if someone asks to be added to any of Sprint’s do not contact lists, Sprint must honor that request. Direct the person to contact Customer Care or to contact Sprint at officeofprivacy@sprint.com.

If you receive any external inquiries about Sprint Nextel’s privacy policy, please reference the public facing privacy policy, located at www.sprint.com. Click on the “Your Privacy Rights” link in the footer.

Customer Authentication

To better protect customer records, the FCC's 2007 CPNI rules require carriers to authenticate their customers before releasing customer information or making changes to a customer's account.

Authentication is the process that you must follow to validate that a customer is who he/she claims to be. Authentication obligations apply to both business and consumer customers.

Customer Authentication Methods*

To comply with the FCC's new rules, Sprint decided to authenticate customers through several methods:

- **PIN**: Customers select their own 6-10 digit numeric PIN. The PIN can be used when calling Sprint Customer Care or visiting a Sprint or dealer retail location.
- **Security Question/Answer**: Customers pick a security question from a preset list (e.g. "What is your first pet's name?") and then provide Sprint with the answer to the question (e.g. "Buddy"). This is used if the customer forgets his/her PIN.
- **Photo ID**: Customers in retail stores can provide a valid, government issued photo ID.
- **Online Username + Password**: Customers that wish to access his/her Sprint account online may do so at www.sprint.com. To access an account online, a customer must establish a username (e.g. sallysmith5) and alpha/numeric password (e.g. apple123).

* *The above procedures apply only to customers who are on the new unified billing platform (UBP) only. For customers still in P2K or other billing systems, legacy authentication procedures apply.*

Customer Authentication Set Up

PIN and security question/answer set up

- **New customers** will be asked to pick a PIN and backup security question/answer (in case you forget your PIN) at the point of sale.
- **Existing customers** will be asked to pick a PIN and backup security question/answer (in case you forget your PIN) soon, if not already, through an internal Sprint channel.

If a Sprint customer does not have a PIN or backup security question/answer, you may authenticate the customer via a valid, government issued Photo ID.

If an existing Sprint customer would like to establish a PIN and backup security question/answer, please direct that customer to contact an internal Sprint Channel, such as Sprint Online (www.sprint.com/PIN).

Customer Notifications

Pursuant to the 2007 FCC CPNI rules, all carriers including Sprint must notify a customer of certain changes to his/her account.

Events that trigger a notification include:

- Change of PIN
- Change of primary means of communication
- Change of security question/answer
- Change of billing address of record

Sprint will send these notifications to one of the customer's "preferred communication" methods (e.g. SMS/Text Message, Email, etc.).

If a customer would like to set or change their "preferred communication method" they may access their account online (www.sprint.com). Once logged in online, click on "Settings and Passwords" and then "Account Access. Postal or email addresses on record with Sprint for at least 30 days are eligible for selection."

Question 4

What is Authentication?

a) The customer contact information set up with Sprint.

b) Another term for identity-theft.

c) A validation process to confirm a person is who they claim to be.

d) A customer's social security or tax id number.

Pick your answer and proceed to the next slide

Question 4 - Answers

a) **Wrong.** The customer contact information is not used for authentication.

b) **Wrong.** Identity theft is a problem where someone gathers enough personal information about another person (e.g. a Sprint customer) to successfully authenticate themselves as that other person.

c) **Correct.** Authentication is a validation process to confirm a person is who they claim to be.

d) **Wrong.** Social security or tax id numbers are personal information, not authentication processes. And, in most instances, neither are used to authenticate Sprint customers.

Please review the answers and then proceed.

Data Theft

Pretexters are bad actors that impersonate Sprint Nextel customers and employees to steal customers' confidential information.

- They target retail stores and Customer Care Reps because they have access to Sprint customer information. They may also target non-customer facing employees with access to customer information.
- Don't bend the rules for seemingly needy or belligerent customers or co-workers.
- Always adhere to Sprint requirements to authenticate the customer's identity before giving account information or changing account PINs/passwords.
  - Insist that the customer provide the authenticating information that company policy requires (e.g. account PIN or valid government issued photo ID that matches the name on the account).
  - Never treat name, address and phone number as sufficient authentication.
- Explain to customers that privacy protection is for their benefit and protects them against others stealing their personal information

Safeguard Customer Records

Sprint Employees must safeguard customer records in their possession / control

Administrative, Physical and Technical Safeguards include:

- Locking and securing retail locations and files/cabinets
- Maintaining files in restricted area
- Restricting access to need-to-know only
- Using unique usernames and passwords for computer access
- Encrypting wireless systems

Record Retention

- Keep customer contracts and supporting documents on site for 1 year. Keep all documents confidential, safe and secure.

- Archive customer contracts and supporting documents that are older than 1 year.

Failing To Comply & Consequences

If you do not adhere to these Policies and Compliance Instructions, you could be disciplined, and Sprint may even terminate its contract with your company.

If you have any questions or concerns about this Policy or the Compliance Instructions or, if you cannot access or you do not understand the Compliance Instructions, please email officeofprivacy@sprint.com.

Sprint Nextel's Privacy Policy

- In addition to the Sprint Do-Not-Contact Policy, Sprint also maintains a customer-facing policy.
- This policy is available at www.sprint.com by clicking on "Your Privacy Rights."
- Link is at the bottom of almost every page on the Sprint Nextel website.
- This policy explains to customers and prospective customers how Sprint Nextel will treat their CPNI and other customer information and how Sprint Nextel will honor any do-not-contact preferences.

Summary - Customer Privacy Do's and Don'ts

- Do access Sprint customer information only to help Sprint customers or to sell Sprint products and services in the same category.
- Don't access Sprint customer information to sell non-Sprint products or services.
- Don't access customer information except as necessary to do your job.
- Do strictly follow company procedures to verify a customer's identity before disclosing account information or changing account PINs/passwords.
- Don't even share customer information with other employees or non-employees/contractors unless they must have that data to perform their jobs.
- Don't share with anyone your user ID and password that allows access to customer information databases.
- Do notify your supervisor immediately if you suspect fraudulent activity on an account or any unauthorized access to, or use of, customer data.

Be on Privacy Alert

You are Sprint Nextel's and its customers' first line of defense against theft/misuse of confidential customer information. Breaches of customer privacy can impose millions of dollars in penalties and business loss, and penalties, termination or criminal liability for individual violators.

- Remember the Privacy Do's and Don'ts.
- If you suspect fraudulent activity on an account, you must notify your supervisor immediately to place a fraud alert on that account.
- If you have any questions or suspect any unauthorized access, use or disclosure of customer information that your direct supervisor can't address, please contact a senior manager in your company.

Congratulations!

You have completed the **What You Need To Know About Customer Privacy and CPNI** course.