The Fundamentals:

Fulfilling the FCC’s Annual CPNI Training Requirements

January 22, 2026 2:00 PM (EST)

Agenda

1. Customer Proprietary Network Information (CPNI) and Why It Matters
2. Use and Disclosure of CPNI
3. Safeguards to Protect CPNI
4. CPNI Data Breach Rules
5. Red Flag Rules Reminder

Polling Question #1

Section 1:
CPNI and Why it Matters

CPNI and Why it Matters

- **CPNI** – Governs the access, use, and disclosure of information about customers obtained by the carrier through the provision of voice service to customers
  - Broadband is currently **not** CPNI
  - Video is **not** CPNI
- CPNI rules protect customer privacy
- CPNI rules promote competition, particularly for services that require access to the underlying telecommunications network
- Carriers that do **not** comply with CPNI rules can face substantial fines from the Federal Communications Commission (FCC)

What is CPNI?

Information about your telecommunications voice services and VoIP (internet phone) services.

- **Customer Plan Information**
  - plan name, number of services, associated features
- **Customer Plan Use**
  - how the customer uses these services
- **Customer Call Detail Records**
  - who was called, time of call, date, and duration of the call initiated/received)
- **Carrier Access Billing Records**
  - calling parties, called parties, and call volumes
- **Customer Presubscribed Interexchange Carrier**
  - the amount a customer was billed by their long distance provider

What is Not CPNI?

Aggregate Customer Information

- Data from a group of customers, which could be CPNI, that has removed any customer identifiers

Subscriber List Information

- Customers' names, addresses, and telephone numbers (including unlisted numbers and non-published numbers)

Examples

Scenario	CPNI?	Why
Sending a postcard to all customers in a ZIP code	❌ No	Uses address only (subscriber list information)
Emailing customers because they are "on an unlimited plan"	✅ Yes	Plan type is CPNI because it reveals the customer's telecommunications service subscription
Offering a new calling plan to "heavy call-volume" customers	✅ Yes	Call-volume level is derived from call detail information, which is CPNI
Ads based on regional customer counts	❌ No	Uses aggregate, de-identified customer information
Segmenting by "customers who called competitors"	✅ Yes	Uses CPNI and is expressly prohibited by FCC rules

Section 2:
Use and Disclosure of CPNI

Section 2: Agenda

1. Restrictions on Use and Disclosure
2. Allowable Uses of CPNI
3. Prohibited Uses of CPNI
4. Use of CPNI in Marketing
5. Customer Approval

Use and Disclosure of CPNI

Restrictions on Use and Disclosure

- In Section 222 of the Communications Act of 1934, as amended, Congress created a framework governing telecommunications carriers' protection and use of information obtained by virtue of providing service
- CPNI has the greatest level of protection under this framework
- Telecommunications carriers can only use CPNI for certain purposes and must take specific steps to ensure CPNI is protected from unauthorized disclosure
- In 2007, the FCC extended these CPNI rules to interconnected Voice over Internet Protocol(iVoIP) providers

Use and Disclosure of CPNI

Allowable Uses of CPNI

- Carriers can use CPNI for the following purposes:
  - Billing and collection
  - Provisioning of voice services
  - Protecting the rights or property of the carrier or protecting users and other carriers from fraudulent, abusive, or unlawful practices
  - Upon affirmative written request by the customer to any person designated by the customer
  - Marketing services to which the customer already subscribes

Use and Disclosure of CPNI

Prohibited Uses of CPNI

- When a carrier receives CPNI from another carrier for billing or provisioning purposes, the CPNI **cannot** be used:
  - For marketing purposes;
  - To retain the customer or engage in retention marketing campaigns, unless the customer has already been lost, in which case the carrier can engage in “win-back” campaigns
- Carriers cannot use CPNI for anti-competitive purposes, such as to identify or track customers who call competitors

Polling Question #2

Use and Disclosure of CPNI

Uses of CPNI in Marketing

- Most carriers no longer need to use CPNI for marketing

- If a customer subscribes to one or more telecom services a carrier offers (Example - local exchange, long distance, or wireless), then the carrier can use CPNI to market service offerings that are part of that telecom service or package of services to which the customer subscribes

- If a customer does **not** subscribe to a telecom or non-telecom service a carrier offers and that carrier wants to use CPNI to market that service, the carrier must first obtain approval from the customer through one or more of the following methods:
  1. Opt-out
  2. Opt-in
  3. Streamlined approval allowed for limited one-time use

Use and Disclosure of CPNI

Customer Approval: Opt-Out Approval

Carriers can use this method to obtain customer approval to use CPNI to market communications-related services provided by a division or affiliate

Carriers using this option must mail notices every other year to their customers giving them the option to opt out and must adhere to certain additional “safeguard” requirements

A customer is deemed to have consented to the use, disclosure, or access to the customer’s CPNI if the customer fails to object within 30 days after the notification is sent (33 days if the notice is mailed)

Use and Disclosure of CPNI

Customer Approval: Opt-In Approval

Under this method, carriers must obtain affirmative, direct consent from the customer allowing the requested CPNI usage, disclosure, or access

Carriers must use the opt-in method if they want to market non-telecom services or share CPNI in a joint arrangement

Use and Disclosure of CPNI

Customer Approval: Streamlined Approval for One-Time Use of CPNI

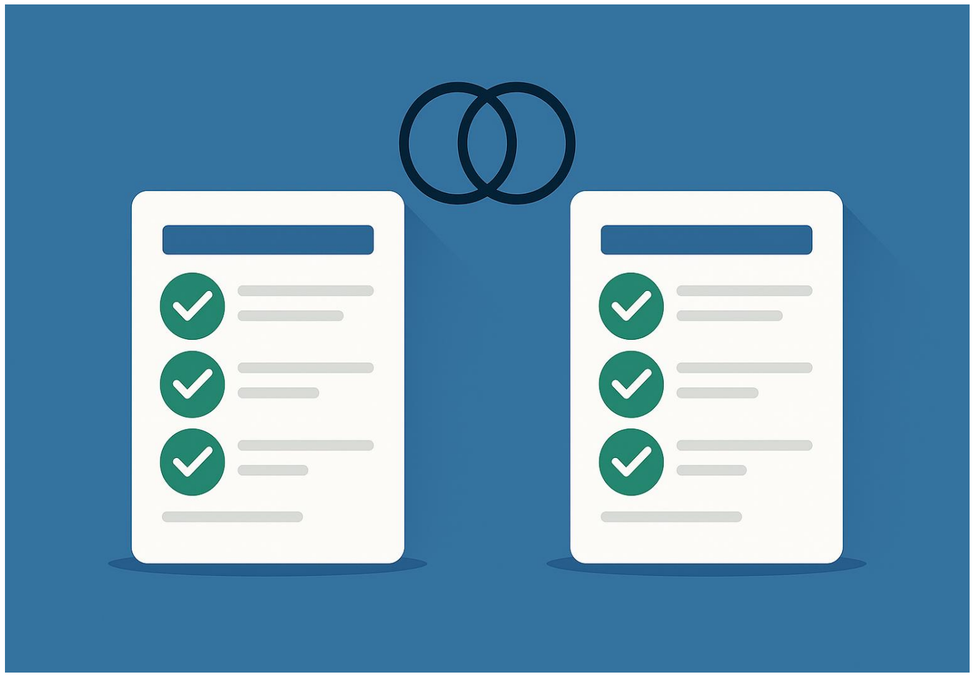
Carriers may orally obtain limited, one-time approval of CPNI use from a customer during an inbound or outbound call

The approval lasts only for the duration of the call

The customer's approval does not change the opt-in or opt-out status

Best practice - Carriers should have a script for employees to use

Comparing Subscriber Lists



- You can compare customer lists to target market customers that do not take certain services without violating the FCC's CPNI rules
- Given this option, most carriers have a policy that states employees will not use CPNI for marketing other services outside of those to which the customer subscribes
- If a carrier has such a policy, then it is not required to send opt-out notices or adhere to the additional safeguard requirements as long as it includes a statement on its annual CPNI certification to that effect

Section 3:
Safeguards to Protect CPNI

Section 3: Agenda

1. Carrier Authentication Requirements
2. Authentication Methods
3. Password Authentication
4. Online Account Access
5. Account Change Notification
6. Training and Record Keeping
7. Annual Certification Filing

Safeguards to Protect CPNI

Carrier Authentication Requirements

- In response to an increase in unauthorized disclosure of CPNI due to data brokers and pretexting, the FCC adopted rules requiring carriers to authenticate a customer's identity before releasing call detail
  - Data Brokers - websites that advertise the sale of personal telephone records
  - Pretexting – third party pretending to be a customer in order to obtain access to that customer's call detail
  - Call Details - any information that pertains to the transmission of specific telephone calls, including the inbound or outbound number and the time, location, or duration of any call
- Most unauthorized releases of call details are through inbound calls

Safeguards to Protect CPNI

Authentication Methods

- Carriers can release call detail to:
  - A customer in person with a valid photo ID
  - A customer who calls in and provides enough call detail information to show they are looking at their bill
- Alternatively, carriers can release call details after verifying a customer's identity through one of the following processes:
  - Calling a customer back at the telephone number of record the carrier has on file (must be on file for at least 30 days)
  - Sending a copy of the bill with call detail information to the address of record (mail or email) the carrier has on file (must be on file for at least 30 days)
  - Establishing a password for the customer to use when calling in with billing questions

Safeguards to Protect CPNI

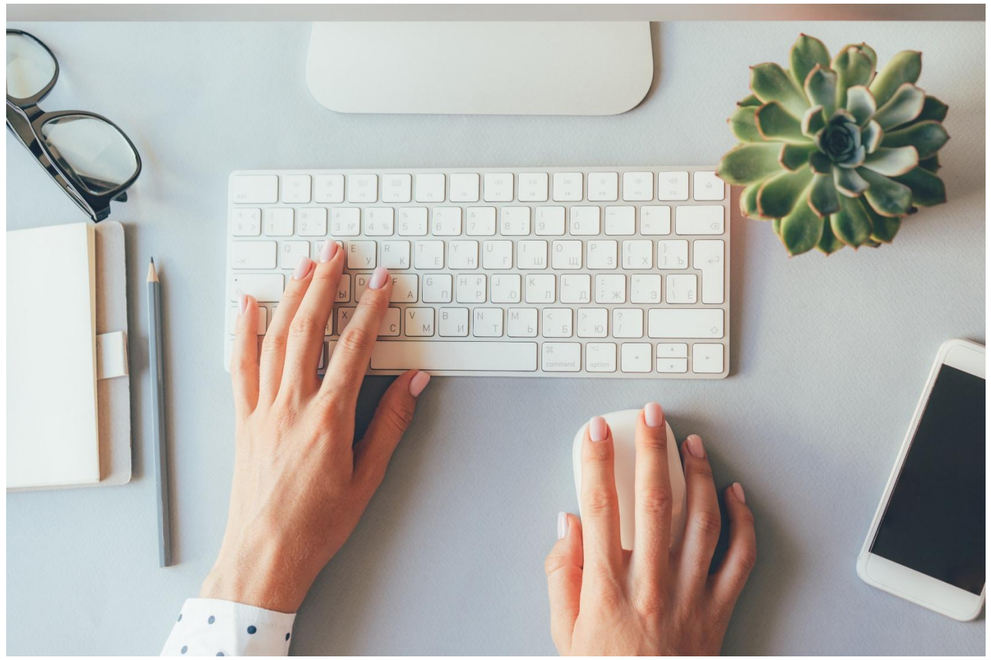
Password Authentication

- Using passwords is considered a best practice for authenticating a customer's identity for inbound calls
- Establishing a password for **new customers** can be done when the customer first signs up for service
- For **existing customers**, carriers can create a password.
  - For example, creating a temporary password that the customer will modify to a password of their choice
- Carriers must obtain and verify a password during customer-initiated calls before releasing any customer call detail
- The password cannot rely on readily available biographical information (ex. SSN, DOB) or account information to validate a customer's identity or to establish "back-up" questions for forgotten passwords.

Safeguards to Protect CPNI

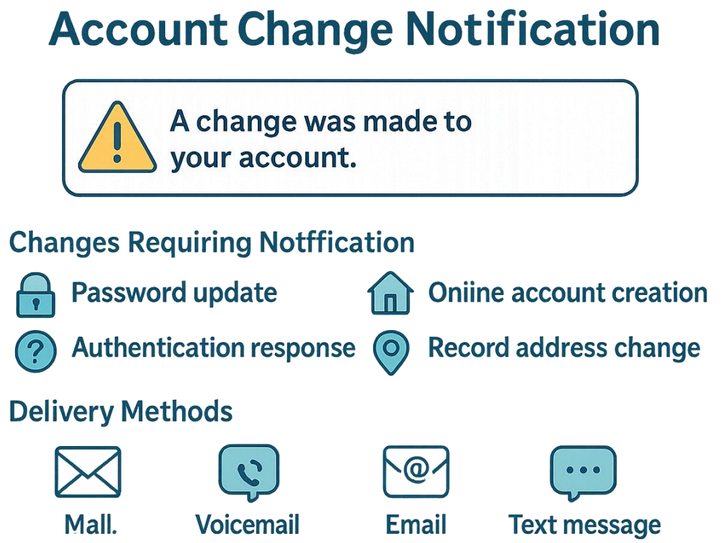
Online Account Access

- Carriers are required to provide password protection for all online account access
- Call detail and non-call detail must be protected by the password
- Carriers cannot base online access solely on biographical or account information



Account Change Notification

- When a change is made to a customer account, carriers are required to notify the customer that a change occurred
  - Notification cannot disclose what account information has changed
- Account changes that require notification include:
  - Create or change passwords
  - Create or change a response to the back-up authentication question
  - Create an online account
  - Change the address of record
- Change Notification Delivery Methods
  - Carriers can notify the customer by mail (to the address of record), voicemail, email, or text message
  - Must be sent to the current address, number, or email of record.



Account Change Notification

- ***Domestic Violence Line Separation Request Exemption*** - Customer notification is **NOT** required if an account change is made in connection with a line separation request under 47 U.S.C. 345 and 47 CFR §64.6400, et. seq. [Victims of Domestic Violence, Human Trafficking, and Related Crimes].

- What is Line Separation?

  - The process that allows a survivor of domestic violence, dating violence, stalking, sexual assault, or human trafficking to move their wireless phone line off a shared or family phone plan that includes an abuser and establish it as a separate, independent account—while keeping their existing phone number.
  - This protection applies even if the survivor is not the primary account holder on the original phone plan.

Polling Question #3

Safeguards to Protect CPNI

Training and Record Keeping

- Carriers must train their personnel on when they are and are not authorized to use CPNI
- Carriers must have an express disciplinary process in place for violations of CPNI use and disclosure rules
- Carriers must maintain a record of all instances where CPNI was disclosed or provided to third parties or where third parties were allowed to access CPNI
- Carriers must retain the record for a minimum of one year

Annual Certification Filing

- Carriers must annually certify CPNI compliance with the FCC on, or before, **March 1st,** for the prior calendar year.
  - A corporate officer, as an agent of the carrier, must sign a certification stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI rules
  - A statement must accompany the certification explaining how the company's operating procedures ensure compliance with the rules
  - A report of any actions (i.e., state petitions, legal action, etc.) taken against data brokers, as well as a summary of customer complaints related to unauthorized release of CPNI received in the prior year must be included

Safeguards to Protect CPNI

Penalties for Non-Compliance

- **Penalty Structure**

  The FCC can impose civil monetary forfeitures for non-compliance, including failure to submit certifications. Base penalties are adjusted annually for inflation per the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015.

  - Per Violation or Per Day of Continuing Violation**:** Up to $251,322.
  - Maximum Aggregate Penalty: $2,513,215 for a single case or series of related violations.

- **Enforcement**
  - In 2023, the FCC proposed a $20 million forfeiture against two mobile providers for CPNI misuse (e.g., weak authentication leading to unauthorized access), highlighting aggressive enforcement.
  - Historical cases show fines ranging from $10,000–$100,000 for initial failures, escalating for repeats.

Section 4:
Data Breach Rules

Existing Data Breach Rules

CPNI Breach Notification

- CPNI Breach - any instance in which a person, without authorization, has intentionally gained access to or disclosed customer proprietary information
  - Carriers must notify both the customer and law enforcement when CPNI is breached
  - Carriers must first send notification electronically to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) within 7 days of determining the breach at: http://www.fcc.gov/eb/cpni
  - The carrier may only notify the customer of the breach publicly 7 business days following the USSS and FBI notifications

Polling Question #4

Pending Data Breach Rules

- On Dec 13, 2023, the FCC updated data breach notification rules for telecom, VoIP, and telecommunications relay services (TRS). New rules ensure customer data protection, enabling customers to protect themselves in the event of a breach.

- When the new rules were published in the Federal Register in February 2024, the only things that went into effect were the changes made to the section titles.

- The effective date for rules in 64.2011 and 64.5111 was “delayed indefinitely”.

DATES:

This rule is effective March 13, 2024, except for the amendments codified at 47 CFR 64.2011 and 64.5111, instructions 3 and 4, respectively, which are delayed indefinitely. The Commission will publish a document in the **Federal Register** announcing the effective dates for the amendments to 47 CFR 64.2011 and 64.5111.

Pending Data Breach Rules

- Expanded scope of a breach to include Personally Identifiable Information (PII) CPNI and PII together are referred to as “Covered Data”

- What is PII?

  - PII is *“information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. CPNI is a subset of PII.”*

Pending Data Breach Rules

- **FCC Further Defines Scope of PII** -

1. first name or first initial, and last name, in combination with any government-issued identification numbers or IDs;

2. user name or e-mail address, in combination with a password or security question and answer, or any other authentication method or information necessary to permit access to an account; or

3. unique biometric, genetic, or medical data.

Pending Data Breach Rules

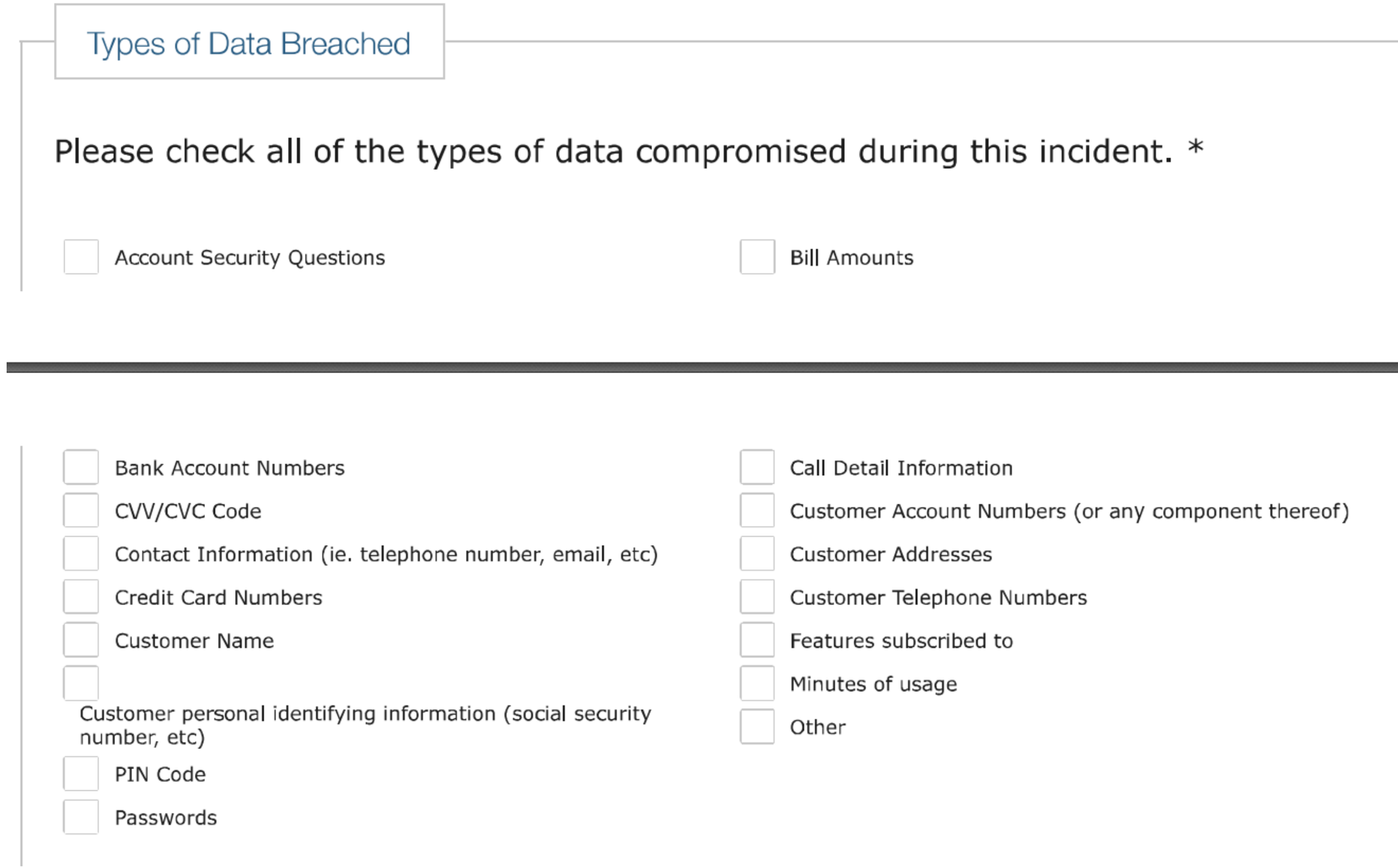
- **What is a Breach?** - any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed covered data.
- New rules expand the definition of breach to include inadvertent access, use, or disclosure of covered data.
- **Good-faith Exception** - good-faith acquisition of covered data by an employee or agent of a carrier where such information is not used improperly or further disclosed.
  - Excluded from definition of breach

Pending Data Breach Rules

- New rule requires notification to FCC as well as the FBI and Secret Service as soon as practicable, but no later than 7 business days
  - Will still use the existing Data Breach Reporting Portal - https://www.cpnireporting.gov
- Eliminates mandatory 7-business-day customer notification waiting period
- Instead, must notify customers no later than 30 days

Pending Data Breach Rules

- Even though these new rules are not yet effective, the FCC's Data Breach Portal is requesting the expanded PII.



Pending Data Breach Rules

- “No Harm” Exception – when the breach impacts less than 500 customers and can reasonably determine that no harm to customers is likely
  - No Harm Annual Reporting – February 1 - a consolidated summary of breaches that occurred over the course of the previous calendar year

- Guidance to determine if a breach would cause harm to customers:
  - Sensitivity of the information (including in totality) that was breached.
  - Nature and duration of the breach.
  - Mitigations.
  - Intentionality.

Pending Data Breach Rules

- Encryption Safe Harbor -
  - Customer notification is not required where a breach solely involves encrypted data, and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed.

Section 5:
Red Flag Rules Reminder

Polling Question #5

The “Red Flag” rules contain 26 “red flags” that indicate the possibility of Identity Theft

Section 111 of the Fair and Accurate Credit Transactions Act of 2003 (“FACT”) Act defines “identity theft” as “a fraud committed using the identifying information of another person, subject to such further definition as the Federal Trade Commission (FTC) may prescribe, by regulation”.

Red Flag Rules

Application of Rule Clarified

- The FTC has determined that even if a company meets the definition of “creditor” it may not be required to comply and provides this guidance:
  - **Ask whether the company regularly and in the ordinary course of business:**

    Gets or uses consumer reports in connection with a credit transaction

    Gives information to credit reporting companies in connection with a credit transaction

    Advances funds to — or for — someone who must repay them, either with funds or pledged property (excluding incidental expenses in connection with the services you provide to them)

- **If you answer:**
  - No to all, the rule does not apply
  - Yes to one or more, the company must comply

Red Flag Rules

Categories of Red Flags

- Alerts, notifications, or warnings from a Consumer Reporting Agency (CRA)
- Suspicious documents
- Suspicious personal identifying information
- Unusual use of, or suspicious activity related to, the covered account
- Notice from customers, victims of identity theft, Law Enforcement Authorities (LEAs), or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor

Red Flags

Companies should be aware of 26 potential red flags when developing their written Identity Theft Prevention Program. Companies are not required to implement all 26 red flags.

1. Fraud alert included with customer report
2. Notice of credit freeze in response to a customer report
3. Address discrepancy in customer reporting agency
4. Unusual credit activity (increase in # of or inquiry of accounts)
5. Authentication documents appear altered or forged
6. Photo on ID inconsistent with appearance of customer

7. Info on ID isn’t consistent with information provided by person opening the account
8. Signature is inconsistent
9. Application appears forged/altered
10. SSN doesn’t match
11. Lack of correlation between SSN and DOB
12. Personal information associated with known fraud
13. Suspicious addresses-mail drop/only PO/Prison
14. SSN is the same as someone else already in your system
15. Address/phone # supplied matches a large group of other applicants
16. Person opening the account is unable to supply identifying information to an incomplete application

17. Personal information is inconsistent with information already on file
18. Unable to correctly answer challenge questions
19. Request for additional users shortly after opening the account
20. Customer fails to make first payment or adds lots of services after the initial set-up in a short period of time
21. Drastic changes in payment patterns
22. Mail repeatedly returned as undeliverable to the address on file
23. Customers say they aren’t receiving paper statements that they asked for
24. Inactive account suddenly becomes very active
25. Notification of unauthorized charges/transactions
26. Notification from the customer that their identity has been stolen

Company's Red Flag Policy

Opening Accounts

- For example:
  - In order for a customer to open an account with the company, the company verifies each customer by requiring the customer to come into the company's customer service office or provide identifying information when calling the company directly to request service and at a minimum provide certain identifying information and documents

Existing Accounts

- For example:
  - The company does not permit customers to access online account information without the use of a password or PIN code that is not prompted by the company asking for readily available biographical information or account information

Monitoring Covered Accounts

- For example:
  - The company monitors transactions associated with its existing accounts by maintaining a secure database containing customer profiles which can be accessed and updated only by appropriate company representatives

Red Flag Rules

Identity Theft Prevention Program

- Under the Red Flag rules, Companies must develop and implement a written Identity Theft Prevention Program. The final regulations list four basic elements that must be included in the written program:
  - Identify Red Flags
  - Detect Red Flags
  - Prevent and Mitigate Identity Theft
  - Update the Program

- Report any identified **red flags** to your supervisor

- Update your Red Flag Manual or Procedures and Contacts

Questions?

Thank you.

Contact Us:

Lans Chase: Lans.Chase@jsitel.com

Leslie Ellis: Leslie.Ellis@jsitel.com