ZIRKEL WIRELESS, INC.
Customer Proprietary Network Information
Compliance Manual

Effective Date: March 1, 2023

The policy of Zirkel Wireless, Inc. ("Zirkel" or "Company") is to comply with all statutes, rules and regulations of the United States. This includes those related to the protection and use of Customer Proprietary Network Information ("CPNI"). Zirkel relies on its management personnel to implement its CPNI policies and procedures to ensure that Company does not use CPNI for any reason until a full review of applicable law has been made.

This Customer Proprietary Network Information Compliance Manual ("CPNI Manual") constitutes Zirkel's policies and procedures related to CPNI. All Company personnel (including management personnel and employees, as well as full-time, part-time and temporary personnel) are required to follow the policies and procedures described in this CPNI Manual. Questions regarding compliance with applicable law or this CPNI Manual should be directed to Company's Compliance Officer.

Zirkel's CPNI Compliance Officer is:

NAME: Joshua Nowak

TITLE: Operations Manager

EMAIL ADDRESS: joshua@zirkel.us

TELEPHONE NUMBER: 970-871-8500;102

TABLE OF CONTENTS

IMPORTANT DEFINITIONS

Account Information. Information that is specifically connected to a customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill amount.

Address of Record. An address, whether postal or electronic, that the carrier has associated with the customer's account for at least 30 days.

Affiliate. A person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. The term "own" means to own an equity interest (or the equivalent thereof) of more than 10 percent.

Aggregate Customer Information. Collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

Breach. When a person, without authorization or exceeding authorization, has intentionally gained access to, used or disclosed CPNI.

Call Detail Information. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Centrex. A telephone service in which a group of phone lines can be joined by part of the local exchange acting as a private exchange.

CMRS. Commercial Mobile Radio Service.

Communications-Related Services. Telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment (CPE).

Company. Zirkel Wireless, Inc.

Customer. A person or entity to which the telecommunications carrier is currently providing service.

Customer Premises Equipment (CPE). Equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.

Emergency Notification Services. Services that notify the public of an emergency.

Emergency Services. 9-1-1 emergency services and emergency notification services.

Emergency Support Services. Information or database management services used in support of emergency services.

FCC. The Federal Communications Commission.

Information Services Typically Provided by Telecommunications Carriers. Information services that telecommunications carriers typically provide, such as Internet access or voice mail services. The term does not include retail consumer services provided using Internet websites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.

Interconnected VoIP Service. A service that: (1) enables real-time, two-way voice communications; (2) requires a broadband connection from the user's location; (3) requires Internet protocol-compatible customer premises equipment; and (4) permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network. For purposes of this CPNI manual, interconnected VoIP is deemed to be a "telecommunications service."

Local Exchange Carrier (LEC). Any person engaged in the provision of telephone exchange service or exchange access. Such term does not include a person insofar as such person is engaged in the provision of a commercial mobile radio service (except to the extent that the FCC determines that such service should be included in the definition of the term).

Opt-In Approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure or access after the customer is provided appropriate notification of the carrier's request consistent with the rules.

Opt-Out Approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the prescribed waiting period, after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules.

Opt-out. A cost-free method that enables a customer to deny, withdraw or revoke his/her consent.

Public Safety Answering Point. The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

Readily Available Biographical Information. Information drawn from the customer's life history and includes, but is not limited to, such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

Subscriber List Information (SLI). Any information (1) identifying the listed names of a carrier's customers and the customers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (2) that the carrier or an affiliate has published, caused to be published or accepted for publication in any directory format. SLI is not classified as CPNI.

Telecommunications Carrier or Carrier. Any provider of telecommunications services, except that such term does not include aggregators of telecommunications services. For purposes of this Manual, the term also includes an entity that provides interconnected VoIP service.

Telecommunications Service. The offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

Telephone Number of Record. The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

Valid Photo ID. A government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable identification that is not expired.

I. OVERVIEW

A. What Is CPNI?

Customer proprietary network information ("CPNI") is data collected about customers by telecommunications carriers such as local, long distance and wireless telephone carriers, and interconnected voice over internet protocol ("VoIP") providers, (collectively "telecom/VoIP providers") by virtue of the provision of those services. CPNI typically includes data about the services that customers subscribe to but also the amount they use those services and in some cases the type of usage. CPNI is often some of the most sensitive information that providers acquire about their customers. For example, CPNI may include the phone number(s) a customer calls, the frequency he/she calls any phone number, the duration and timing of such calls, and any services purchased by a customer like call forwarding, call blocking or voicemail. Furthermore, CPNI may individually identify customers to third parties such as hackers or marketers as it also includes account and payment information.

Congress has recognized that a telecom/VoIP provider like Zirkel is in a unique position to obtain sensitive personal information about its customers. Congress also recognized that customers maintain an important privacy interest in not having this information disclosed or disseminated. Congress codified this interest in section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, 47 U.S.C. § 222. Section 222 requires that telecommunications carriers take steps to safeguard CPNI from unauthorized or accidental access, use, or disclosure. The FCC extended these statutory requirements to govern interconnected VoIP providers in 2007.

The FCC requires that telecom/VoIP providers protect this personal information through the establishment of systems and reasonable procedures designed to safeguard this data including but not limited to specific requirements for authenticating customers, securing customer approval for use of CPNI under certain circumstances, training all Company personnel to recognize when CPNI use is authorized and when it is not authorized, and creating a disciplinary process to address deviations from Company policy.

Risks involved with unauthorized access, use or disclosure of CPNI by Company personnel, Company affiliates, agents, joint venture partners or independent contractors include identity theft, physical harm or stalking, and exposure to hackers and data brokers. Failure to comply with the FCC's CPNI rules, including the annual certification requirement, can result in substantial fines up to $2,000,000 for a single violation depending on the circumstances.

B. Zirkel Objectives

1. Reasonably protect the personal and sensitive personal information of Company customers.

2. Limit ability of any unauthorized person to access, use or disclose CPNI.

3. Secure customer Opt-In Approval or Opt-Out Approval when appropriate and honor customer's request to deny, revoke or withdraw his/her consent (i.e., opt-out) for marketing and promotional purposes.

C. Use Of CPNI In General

Zirkel has a duty to protect the CPNI of its customers. Except as otherwise stated in this CPNI Manual, when Zirkel obtains any CPNI through its provision of telecommunications services it may only use, disclose or permit access to that CPNI for the provision of (1) telecommunications service from which the information is derived or; (2) services necessary to provide, or used in the provision of, telecommunications services.

1. Company will not sell CPNI to any unaffiliated third party for marketing or promotional purposes.

2. When Company receives or obtains CPNI from another Telecom/VoIP provider for purposes of providing any telecommunications service, it will only use the CPNI for that purpose, and not for Company's own marketing efforts.

3. Company will only use, disclose, or permit access to aggregate customer information, if the information is provided to other Telecom/VoIP providers or persons on reasonable, nondiscriminatory terms and conditions upon reasonable request.

4. Company will not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers.

II. CPNI USE OVERVIEW

A. CPNI Uses That Do Not Require Customer Approval

1. Company may use, disclose or permit access to CPNI without customer consent in its provision of the following **delivery of service** purposes:

   a. Inside wiring installation, maintenance, and repair services.

   b. To protect the Company's rights or property, to protect customers, or other Telecom/VoIP providers from fraudulent, abusive, or unlawful use of, or subscription to such services.

   c. To use, disclose or permit access to CPNI for the purpose of providing service offerings among the categories of service (*i.e.,* local, interexchange, and CMRS) to which the customer already subscribes from the Company.

   d. If Company provides different categories of service, and a customer subscribes to more than one category of service offered by the

Company, the Company may share CPNI among the Company's affiliated entities and agents that provide the service offerings to the customer.

2. Company may use, disclose or permit access to CPNI **without** customer consent in its provision of the following **marketing** purposes:

   a. To use, disclose or permit access to CPNI for the purpose of the Company marketing service offerings among the categories of service (*i.e.,* local, interexchange, and CMRS) to which the customer already subscribes to from the Company.

   b. To market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding and certain centrex features.

EXAMPLE:

Customer subscribes to the local telephone service and long distance service of ABC Teleco Inc. ("ABC"). ABC may share customer CPNI with its affiliated entity, YXZ Corp., that assists ABC with providing a service offering to the customer.

IMPORTANT NOTE:

A customer has the right to opt-out of any marketing use of CPNI by the Company, its affiliates, agents, joint venture partners or independent contractors for marketing purposes at any time and at no cost to the customer.

B. CPNI Uses That Require Customer Approval (Opt-In Or Opt-Out Approval)

1. **Opt-In Approval**:

   a. Company's access, use, or disclosure of CPNI for its purpose of marketing new or non-communications-related service offerings provided by the Company.

   b. Company's disclosure of CPNI to affiliated entities if Company provides different categories of service but customer only subscribes to one service offering.

   c. Except as required by law, Company's disclosure of CPNI to third parties, or to Company's own affiliates and agents that do not provide communications-related services.

EXAMPLE:

Customer subscribes to local telephone service of ABC Teleco. Inc. ("ABC"), but no other service. ABC is prohibited from sharing customer's CPNI with its affiliate, XYZ Inc. that provides long distance service without obtaining customer's prior express Opt-In Approval.

d. Company's disclosure of CPNI to joint venture partners or independent contractors for the purpose of marketing communications-related or non-communications-related services to Company's customer.

2. **Opt-Out** Approval:

a. Company's disclosure of CPNI to its agents or its affiliated entities that provide communications-related services to the customer for the agents or affiliated entities' own marketing of communications-related services.

b. Company's one-time use of CPNI for inbound or outbound customer telephone communications only for the duration of the call. (See Sec. IV(D), herein for details.)

III. CUSTOMER OPT-IN APPROVAL AND OPT-OUT APPROVAL METHODS

A. Requirements For Systems And Procedures Regarding Customer Approval

1. Company must establish and implement a system and procedures by which the status of a customer's CPNI approval can be clearly established prior to the use of the CPNI.

a. Opt-In Approval is secured by a customer's affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided the appropriate notification set forth in Sec. IV, herein.

b. Opt-Out Approval is secured when a customer has failed to object within the minimum thirty (30) calendar day waiting period after the customer is provided the appropriate notification set forth in Sec. IV, herein.

2. Company may seek approval for the use of CPNI through solicitation of customers via written, oral, or electronic methods. If the Company relies on oral approval, it bears the burden of proving that approval has been given in accordance with FCC regulations.

3. Regardless of the approval method, a customer's approval or disapproval to use, permit access or disclose CPNI must remain in effect until the customer revokes or limits such approval or disapproval. Company must maintain a record of customer approval for at least one (1) year.

4. Company must first obtain, express, verifiable, prior approval from customers to send notices via email regarding its service in general, or CPNI in particular.

   a. If email is used to send CPNI-related notices, Company must ensure that the subject line of the message clearly and accurately identifies the subject matter of the email.

   b. Customers must be allowed to reply directly to emails containing approval notices in order to respond to Opt-Out Approval request for any proposed access, use or disclosure of CPNI.

   c. Opt-Out Approval email notices that are returned as undeliverable must be sent to the customer in another form before Company may consider the customer to have received notice.

   d. Company must provide notice to the FCC within five (5) business days of any instance where Company's Opt-Out Approval opt-out mechanisms do not work properly, such that a customer's inability to deny consent is more than an anomaly.

      i. Notice to the FCC must be given even if the Company offers more than one method of opting-out.

      ii. Notice to the FCC must be in the form of a letter and include the Company name, a description of the mechanism used, the problem experienced, the remedy proposed and the date it will be/was implemented, whether any relevant state authorities have been notified (and if the state authorities have taken any action), a copy of the notification(s) provided to customers, and Company contact information.

B. Additional Requirements For Disclosure Or Provision Of CPNI To Joint Venture Partners Or Independent Contactors

If Company discloses or provides CPNI access to a joint venture partner or independent contractor or, in addition to customer Opt-In Approval, Company must also enter into a confidentiality agreement with each partner or contractor. The agreement must, at minimum:

1. Require the joint venture partner or contractor to use the CPNI only for the purpose of marketing or providing the communications-related services for which Company has provided the CPNI.

2. Prohibit the joint venture partner or contractor from using, allowing access, or disclosing CPNI to another party except under force of law.

3. Require the joint venture partner or contractor to have appropriate administrative, technical and physical protective measures in place to ensure ongoing confidentiality of Company's CPNI.

4. Require the written agreement by and between Company and joint venture partners or contractors to include additional Company-required provisions to ensure protections of CPNI (such as personnel training requirements) and specific representations and warranties plus indemnification provisions to protect Company.

IV. CUSTOMER OPT-IN APPROVAL AND OPT-OUT APPROVAL NOTICE REQUIREMENTS

A. Requirements For Customer Notification Content And Notification Process

Zirkel must notify customers, prior to any solicitation for customer approval, that the customer has the right to restrict use, access, or disclosure to that customer's CPNI. This notification must provide sufficient information to enable the customer to make an informed decision whether or not to permit Zirkel, or its affiliates, agents, joint venture partners or independent contractors to use, disclose, or permit access to customers' CPNI.

1. All customer notifications:

   a. Must clearly state that the customer has a right and Zirkel has a duty under federal law to protect the confidentiality of CPNI.

   b. Must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which the CPNI will be used, and inform the customer of his/her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

   c. Must advise the customer of the precise steps the customer must take in order to grant or deny access to his/her CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes.

   d. Must be comprehensible and must not be misleading.

   e. Must be clearly legible, use sufficiently large type, and conspicuously placed in an area readily apparent to a customer if the notice is in written form. These same requirements may also apply to electronic forms.

   f. Must be translated into another language in its entirety if any portion of the notification is translated into that foreign language.

g. Must not include any statement attempting to encourage a customer to deny or freeze third-party access to CPNI.

h. Must be proximate to Company's solicitation for customer approval.

2. Customer notifications **may**:

a. Include a brief statement, using clear and neutral language, describing the consequences resulting from the lack of access to CPNI.

b. State that the customer's approval to use CPNI may enhance Company's ability to offer products and services tailored to the customer's needs.

c. State that Company is compelled to disclose CPNI to any person upon affirmative written request by the customer.

3. Company must maintain records of customer notification, whether it be oral, written or electronic, for at least one (1) year.

B. Notice Requirements Specific To Obtain Opt-In Approval

Company may provide notification to obtain Opt-In Approval through oral, written or electronic methods depending on the nature of the approval.

C. Notice Requirements Specific To Obtain Opt-Out Approval

1. Company must provide notification to obtain Opt-Out Approval through electronic or written methods, but not oral methods, EXCEPT as allowed for notice requirements specific to one-time use of CPNI during inbound or outbound telephone communications as detailed in Sec. IV(D), herein.

2. Company must wait at least thirty (30) calendar days after giving a customer an Opt-Out Approval notice, and ample opportunity to opt-out prior to assuming approval to use, disclose, or permit access to CPNI.

3. Company must notify customers as to the applicable waiting period for a response before approval is assumed.

a. For electronic notification (i.e., email) this waiting period commences from the date on which the notification was sent.

b. In the case of written notification sent via postal mail, it commences the third day after the notice was mailed.

4. If Company uses Opt-Out Approval notification it must provide notice every two (2) years.

5. If Company choses to use e-mail to provide Opt-Out Approval notification it must comply with the following additional requirements:

   a. Company must have express, verifiable prior approval from customers to send notices via email regarding their service in general, or CPNI in particular.

   b. Customers must be able to reply directly to e-mail notification in order to complete their denial (i.e., opt-out) of Company's Opt-Out Approval.

   c. If an email notice is returned as undeliverable, the notice must be sent to the customer in another form before Company can consider the notice received.

   d. The email subject line must clearly and accurately identify the subject matter of the email.

6. Company must make available to every customer some method to opt-out that is of no additional cost and available 24 hours a day, seven days a week.

7. Company may satisfy this opt-out requirement through a variety of methods including a combination of methods as along as customers may effectuate their choice to deny any proposed access to CPNI at no additional cost, any time they choose.

D. Notice Requirements Specific To One-Time Use Of CPNI

1. Company may obtain limited one-time use of CPNI for inbound or outbound customer telephone communications only for the duration of the call. This one-time use notification must abide by the notice requirements above, but may omit the following if not relevant for this limited CPNI use:

   a. Company does <u>not</u> need to advise customers that if they opted-out previously no additional action is needed to maintain that opt-out.

   b. Company need <u>not</u> advise that it may share CPNI with its affiliate(s) or third parties and need not name those entities, as long as the limited CPNI use will not result in use or disclosure to an affiliate or third-party.

   c. Company need <u>not</u> disclose how a customer can deny or withdraw future access to CPNI, as long as Company or its agent explains to the customer the scope of the approval for the limited one-time use.

   d. Company may <u>omit</u> a recitation of the precise steps a customer must take to grant or deny access to CPNI, as long as Company or its

agent clearly communicates that the customer can deny access to CPNI for the one-time use call.

V. SAFEGUARDS FOR ACCESS TO AND USE OF CPNI

A. Zirkel Training Requirements

1. Company must train all personnel as to when they are and are not authorized to access or use Company CPNI.

    a. All existing personnel and any new personnel must review this CPNI Manual and indicate in writing that they have read, understand and accept the policies and procedures herein. New personnel must receive this CPNI Manual and required training no later than thirty (30) days after his/her start date, but prior to any access to CPNI.

    b. Training will be provided by the Company's Compliance Officer or his/her designee and/or Company's legal counsel or consultant on a regular basis.

    c. [INSERT COMPANY POLICY REGARDING FREQUENCY OF TRAINING].

2. Company should also require in writing regular training for any personnel of its affiliates, agents, joint venture partners and independent contractors that have access to Company CPNI.

B. Requirements To Consult With Company Compliance Officer Prior To Use Of CPNI

Company personnel will make no decisions regarding the use of CPNI without first consulting Company's Compliance Officer at joshua@zirkel.us.

1. Any proposed use of CPNI by Company personnel must be reviewed and approved by the Compliance Officer.

2. The Compliance Officer's supervisory review will include consultation of this CPNI Manual, applicable laws and FCC regulations, and with legal counsel, if necessary.

3. The Compliance Officer is responsible for overseeing the use of approval methods and notice requirements for compliance with all applicable statutory and regulatory requirements.

4. The Compliance Officer is responsible for ensuring that Company enters into written confidentiality and service agreements with any joint venture partner or independent contractor to whom it discloses or provides access to any CPNI.

C. Company Disciplinary Measures For Improper Use Of CPNI

Improper use of CPNI by any Company personnel will result in disciplinary action in accordance with established Company disciplinary policies, including a written warning, suspension or up to immediate termination. Under limited circumstances, any personnel that has made, or is reasonably believed to have made improper use of CPNI or has violated the guidelines of this CPNI Manual, will undergo additional training to ensure future compliance.

VI. SAFEGUARDS FOR DISCLOSURE OF CPNI

A. Required Security Measures To Protect CPNI

Company must take reasonable administrative, technical and physical measures to detect and prevent attempts to gain unauthorized access to CPNI. This includes properly authenticating customers prior to disclosing any CPNI on customer-initiated phone calls, password protecting online account access, and requiring valid identification during in-store visits.

B. Required Password Protections and Secured Disposal Measures

Company must password protect all propriety databases and equipment that contain CPNI.

1. Access to these databases, equipment and passwords should be restricted to authorized personnel only.

2. Passwords should be changed on a routine basis and immediately when personnel with access to any database containing CPNI leaves the Company.

3. No CPNI should be removed from Company offices. This includes laptops and other PDAs, or thumb and flash drives that contain or allow access to CPNI.

4. CPNI should be deleted in a reasonably secure manner (i.e., burn, pulverize or use of cross-cut shredder for paper files and/or erase, destroy or wipe clean for electronic files so that the CPNI cannot be read or reconstructed) after no more than three (3) years after a customer discontinues service. This includes CPNI contained in paper or electronic back-up files, whether located on the Company premises or at an off-site storage facility.

C. Required Customer Authentication Procedures

Customers seeking access to any CPNI must be authenticated prior to Company allowing access to a telecom/VoIP account. Proper authentication cannot rely on any readily available biographical information, or account information.

1. Customers seeking access to CPNI **online** must first provide Company a password, which was assigned or created without the use of any readily available biographical information.

2. Customers seeking access to CPNI via a **customer-initiated telephone call** must first provide Company with a password that was assigned or created without the use of any readily available biographical information.

3. Customers may access CPNI **in-person** at a retail store, however, customers are required to provide a valid non-expired government-issued photo ID before Company's agent may disclose any CPNI. Customer should not be required to provide a password due to the high risk of public disclosure.

D. Required Measures If Customer Is Unable To Provide Password

1. Company may discuss CPNI with a customer without a password on a customer-initiated phone call but **only** if that customer discloses call detail information unprompted and without Company's assistance.

2. If the customer is unable to provide the correct password, Company may still disclose CPNI, but must provide the information only by sending it to the customer's postal address on file or by calling the customer via the telephone number on file.

3. Company must also establish a password back-up authentication method for lost or forgotten passwords, such as a shared secret question or series of questions. Back-up authentication methods may not use readily available biographical information. If a customer cannot provide the correct response to the back-up customer authentication method, the customer must establish a new password as required herein.

    i. ZIRKEL authenticates users by validating the name on account, phone number on account, and the last 4 digits of the autopay card they have on file.

VII. RECORDKEEPING REQUIREMENTS

A. Requirements To Maintain Records Of Sales And Marketing Campaigns

Except as otherwise specifically specified in this CPNI Manual, Company must maintain records of all sales and marketing campaigns that use CPNI for at least one (1) year. These files must be clearly identified. Records must include the following:

1. Description of each campaign;

2. The specific entity that used CPNI (e.g., Company, agent or affiliated entity);

3. Specific CPNI that was used in the campaign; and

4. Products and services that were offered as part of the campaign.

B. Requirements To Maintain Records Of Disclosure Or Provision Of CPNI To Other Third Parties

Company must maintain records of any instances where it discloses or provides CPNI to any third-party, including but not limited, to joint venture partners, independent contractors, and vendors/agents. Records must include:

1. The specific entity that received CPNI (e.g., type of entity and name);

2. Specific CPNI that was disclosed; and

3. Purpose of the use of CPNI.

C. Requirements For Annual CPNI Certification To FCC

On an annual basis, Company must file a compliance certification with the FCC's Enforcement Bureau on or before **March 1** for the previous calendar year. The annual certification filing must include all of the elements listed below:

1. A compliance certificate signed by an authorized officer of the Company. (See Attachments A & B)

2. A statement by the officer in the compliance certificate that he or she has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the CPNI rules. (See Attachment B)

3. A written policy statement accompanying the certification explaining how the Company's operating procedures ensure that it is or is not in compliance with the CPNI rules. (See Attachment C)

4. An explanation of any actions taken against data brokers. (See Attachment C)

5. A summary of all consumer complaints received in the prior year concerning unauthorized release of CPNI. (See Attachments C & G)

VIII. CPNI SECURITY BREACHES

A. Requirements For Notification To FCC and Law Enforcement In The Event Of Security Breach Of CPNI

In the event of any unauthorized access or reasonable belief that there has been unauthorized access of its customers' CPNI, Company must notify the FCC, the United

States Secret Service ("USSS") and Federal Bureau of Investigation ("FBI") in accordance with the following requirements:

1. Company shall not notify its customers or disclose publicly there has been a breach, until it has properly notified the federal law enforcement agencies identified above.

2. As soon as practicable but no later than seven (7) business days after a reasonable determination of a breach, Company must electronically notify the USSS and FBI using the following website: https://www.cpnireporting.gov.

3. Company must maintain a record of any breaches discovered or notifications made to the USSS or FBI. This record must include dates of discovery and notification, a detailed description of the CPNI that was subject of the breach, and the circumstances surrounding the breach. This record must be maintained for a minimum of two (2) years.

4. [INSERT FCC NOTIFICATION PROCEDURES AND ONLINE PORTAL LINK, ONCE NEW RULES ARE ADOPTED.]

B. Requirements For Notification To Customer In The Event Of Security Breach Of CPNI

Company must notify its customers of a breach of customers' CPNI **only after** it has completed the requirements associated with notifying federal law enforcement agencies, and **not before seven (7) business days** following the reasonable determination of a breach.

1. If Company believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise permitted in order to avoid immediate and irreparable harm, it must note that on its notification to federal law enforcement and may proceed to immediately notify affected customers after consultation with the investigating federal agency.

2. The investigating federal agency may determine that public disclosure may impede or compromise an ongoing investigation. The federal agency may direct Company not to disclose the breach for an initial period of up to thirty (30) calendar days. This delay may be extended by the investigating agency. Company must cooperate with the investigating agency's request.

# # #

Helpful Resources:
Annual Certification Portal: https://apps.fcc.gov/eb/CPNI/

FCC Small Business CPNI Compliance Guide, DA-08-1321 (rel. June 6, 2008): https://www.fcc.gov/document/customer-proprietary-network-information-cpni

https://www.cpnireporting.gov

ANNUAL CPNI CERTIFICATION INSTRUCTIONS

Filing Instructions

The Certificate of Compliance with the FCC's CPNI rules must be filed annually on or by March 1 each year relating to the prior calendar year.

Filing the certificate is not enough. [COMPANY] must make sure that it engages in the practices discussed in the Certificate before signing and filing it.

The certificate must be signed by an officer (i.e. President, Vice President, Secretary) of the Company. The Officer is certifying that he or she has *personal knowledge* that [COMPANY] has established operating procedures that are adequate to ensure compliance with the FCC's CPNI regulations, along with:

- A statement accompanying the certificate to explain how [COMPANY]'s operating procedures ensure they are (*or are not*) in compliance with the rules.
- An explanation of any actions taken against data brokers in the prior year. **If there were no such actions, *include an affirmative statement* of that fact to make clear the required information has been provided**; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. ***If there were no such* complaints, *include an affirmative statement* of that fact to make clear the required information has been provided.**

Electronic Paperless Filing

The Commission's web-based application specifically designed for this purpose is available here: CPNI Template Submission (fcc.gov) (https://apps.fcc.gov/eb/CPNI/). Instructions are provided at the website.

Certifications may also be filed using the Commission's Electronic Comment Filing System (ECFS). To file a certification using ECFS, visit ECFS New Filing (fcc.gov) (https://www.fcc.gov/ecfs/filings).

- Filings submitted through ECFS must reference EB Docket No. 06-36 in the "Proceeding" field.

- Companies with affiliates in possession of a unique 499 filer ID number must file a separate certification.

Do not send copies of certifications to the Enforcement Bureau or to any individuals within the Enforcement Bureau unless such filing is a requirement of a consent decree with the Enforcement Bureau.

ATTACHMENT B

ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION
EB Docket No. 06-36

Annual Section 64.2009(e) CPNI Certification for 20__ covering the prior calendar year 20__.

1. Date filed: February __, 20__

2. Name of company covered by this certification: Zirkel, Inc.

3. Form 499 Filer ID: [ADD]

4. Name of signatory: [ADD]

5. Title of signatory: [ADD]

6. Certification:

I, [SIGNATORY], certify that I am an officer of the company named above and, acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in Section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____,
[SIGNATORY NAME AND TITLE]

Attachment: Statement Explaining CPNI Procedures

Zirkel, Inc.

STATEMENT OF POLICY IN TREATMENT OF CUSTOMER PROPRIETARY NETWORK INFORMATION

The purpose of this Policy Statement is to memorialize the policy of Zirkel, Inc. ("Carrier") on the use and protection of Customer Proprietary Network Information ("CPNI").

1. It is the Carrier's policy not to use CPNI for any activity other than permitted by law. Any disclosure of CPNI to other parties (such as affiliates, vendors, and agents) occurs only if it is necessary to conduct a legitimate business activity related to the services already provided by the Carrier to the customer. If the Carrier is not required by law to disclose the CPNI or if the intended use does not fall within one of the carve outs, the Carrier will first obtain the customer's consent prior to using or disclosing CPNI.

2. Carrier follows industry-standard practices to prevent unauthorized access to CPNI by a person other than the customer or Carrier. However, Carrier cannot guarantee that these practices will prevent every unauthorized attempt to access, use, or disclose personal information. Therefore:

    A. If an unauthorized disclosure were to occur, Carrier shall provide notification of the breach within seven (7) days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI").

    B. Carrier shall wait an additional seven (7) days from its government notice prior to notifying the affected customers of the breach.

    C. Notwithstanding the provisions in subparagraph B above, Carrier shall not wait the additional seven (7) days to notify its customers if Carrier determines there is an immediate risk of irreparable harm to customers.

    D. Carrier shall maintain records of discovered breaches for a period of at least two (2) years.

3. All pertinent personnel (including employees and management) will be trained as to when they are, and are not, authorized to use CPNI upon employment with the Carrier and annually thereafter.

    A. Specifically, Carrier shall prohibit its personnel from releasing CPNI based upon a customer-initiated telephone call except under the following three (3) circumstances:

        1. When the customer has pre-established a password.

        2. When the information requested by the customer is to be sent to the customer's address of record, or

3. When Carrier calls the customer's telephone number of record and discusses the information with the party initially identified by customer when service was initiated.

B. Carrier may use CPNI for the following purposes:

- To initiate, render, maintain, repair, bill and collect for services;
- To protect its property rights; or to protect its customer or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
- To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
- To market additional services to customers that are within the same categories of service to which the customer already subscribes;
- To market services formerly known as adjunct-to-basic services; and
- To market additional services to customers with the receipt of informed consent via the use of opt-in or opt-out approval, as applicable.

4. Prior to allowing access to Customers' individually identifiable CPNI to Carrier's joint venturers or independent contractors, Carrier will require, in order to safeguard that information, their entry into both confidentiality agreements that ensure compliance with this Statement and shall obtain opt-in consent from a customer prior to disclosing the information. In addition, Carrier requires all vendors, joint venturers, contractors, and agents to acknowledge and certify that they may only use CPNI for the purpose for which that information has been provided.

5. Carrier requires express written authorization from the customer prior to dispensing CPNI to new carriers, except as otherwise required by law.

6. Carrier does not market, share or otherwise sell CPNI information to any third party unless it has secured customer opt-in or opt-out approval, as applicable.

7. Carrier maintains a record electronically or in some other manner, of its own and its affiliates' sales and marketing campaigns that use Carrier's customers' CPNI. Carrier shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record will include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. Carrier shall retain the record for a minimum of one (1) year.

A. Prior commencement of a Carrier's sales or marketing campaign that utilizes CPNI, Carrier establishes the status of a customer's CPNI approval. The following sets forth the procedure followed by Carrier.

- Prior to any solicitation for customer approval, Carrier will notify customers of their right to restrict the use of, disclosure of, and access to their CPNI.

- Carrier will use either opt-in or opt-out approval for specific instances in which Carrier must obtain customer approval prior to using, disclosing, or permitting access to CPNI as required by the FCC's rules.

- A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.

- Records of approvals are maintained for at least one (1) year.

- Carrier provides individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.

- The content of Carrier's CPNI notices comply with FCC rule 64.2008 (c).

8. Carrier has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes when such approval is required by the FCC's rules. This system allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.

9. Carrier has a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and will maintain compliance records for at least one (11) year. Specifically, Carrier's sales personnel will obtain express approval of any proposed outbound marketing request for customer approval of the use of CPNI by the Carrier's General Counsel or Legal Representative.

10. Carrier notifies customers immediately of any account changes, including address of record, authentication, online account, and password related changes.

11. Carrier may negotiate alternative authentication procedures for services that Carrier provides to business customers that have a dedicated account representative and a contract that specifically addresses Carrier's protection of CPNI.

12. Carrier is prepared to provide written notice within five (5) business days to the FCC of any instance where the opt-out mechanisms do not work properly to such a degree that consumer's inability to opt-out is more than an anomaly**.**

ATTACHMENT D

[LOGO]

Employee Verification Statement

I, _____, have reviewed and am familiar with [COMPANY]'s CPNI Policy ("Policy"). I understand the obligations the rules imposed on me to protect customer information and I agree to report any violation of that Policy.

I have been given a copy of [COMPANY]'s *Customer Proprietary Network Information Compliance Manual* and I agree to comply with the procedures set forth therein.

I have been made aware and understand that disciplinary action may be taken if I fail to abide by the policies and procedures set forth in the *CPNI Compliance Manual*.

DATE: _____ _____

Employee Signature

OPT-OUT NOTICE

Zirkel, Inc. ("Company") utilizes Customer Proprietary Network Information ("CPNI") when providing telecommunications products and services to its customers. CPNI is defined as information relating to the quality, technical configuration, destination, and amount of use of telecommunications services, including information that may appear on a customer's bill. Information published in the telephone directory is not CPNI.

Under Federal law, telephone companies have a duty to protect CPNI. As a customer, you have the right at any time to restrict the use of CPNI. The Company is requesting to share your CPNI under the "opt-out" approach. Your approval to use CPNI may enhance the Company's ability to offer products and services tailored to your needs.

The Company proposes to use your CPNI to [Specify: (1) the information that will be used, (2) the specific entities that will receive the CPNI, (3) the purposes for which CPNI will be used].

If you wish to opt-out, write to the Company at [INSERT ADDRESS] or send a fax to [INSERT FAX TELEPHONE NUMBER]. A written request is the best and most effective way to place your request.

Your decision to opt-out will not affect the provision of any services to which you subscribe. The Company does not and will not sell or offer such information to any third party, except as permitted under Federal Communications Commission regulations. Once you opt-out, you will remain opted-out until your request otherwise.

If the Company does not receive an opt-out from you prior to the expiration of the 30-day period following the Company's sending of this notice to you, it will assume that you approve of its proposed use of your CPNI.

Customer Proprietary Network Information
Grant of Permission to Disclose CPNI to Third Party

Pursuant to the requirements of Section 222 of the Communications Act of 1934, as amended, and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules), [COMPANY] is unable to provide any information regarding your account to any other party without your express written permission to do so.

Your Account Billing Name: _____
Your Account Billing Address: _____
Your Billing Telephone Number(s):_____

I give my written permission to allow _____, whose address and phone number is _____; (___) _____, to receive written, and/or electronic responses for the following information on the above stated account (describe):

Signature: _____
Printed Name_____

Date: _____

You may revoke this Grant of Permission by writing *or* calling the Company at:

[Complete company address and phone number]

For Company Use Only:

Customer did one of the following:

___ Requested Call Detail Information, presented a Valid Photo ID, and established a password.

___ Requested Call Detail Information and provided password.

___ Requested CPNI other than Call Detail Information and provided password.

___ Requested CPNI other than Call Detail Information, and presented a Valid Photo ID.

___ Requested CPNI other than Call Detail Information and was authenticated by a Company representative calling the customer's Telephone number of record.

CUSTOMER COMPLAINTS ACTIVITY

COMPANY NAME:_____

Complaint Date	Affected Customer Name	Description of Complaint