KELLEY DRYE & WARREN LLP

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400

3050 K STREET, NW

WASHINGTON, DC 20007

(202) 342-8400

NEW YORK, NY
LOS ANGELES, CA
HOUSTON, TX
AUSTIN, TX
CHICAGO, IL
PARSIPPANY, NJ
STAMFORD, CT
BRUSSELS, BELGIUM

AFFILIATE OFFICE
MUMBAI, INDIA

FACSIMILE
(202) 342-8451
www.kelleydrye.com

DIRECT LINE: (202) 342-8614
EMAIL: dsmith@kelleydrye.com

March 1, 2018

VIA ECFS

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554

Re: Annual Customer Proprietary Network Information Compliance Certification, EB Docket No. 06-36

Dear Secretary Dortch:

On behalf of New Century InfoComm Tech. Co. Ltd. ("New Century") and pursuant to 47 C.F.R. § 64.2009(e), attached please find New Century's 2018 Annual Customer Proprietary Network Information compliance certification covering calendar year 2017.

Please contact the undersigned at (202) 342-8612, if you have any questions regarding this filing.

Respectfully Submitted,

Counsel to New Century InfoComm Tech. Co. Ltd.

Annual Customer Proprietary Network Information Certification
Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36
Mar 1, 2018

Name of Company: New Century InfoComm Tech. Co. Ltd.
Form 499 Filer ID: 823102
Annual 64.2009(e) CPNI Certification for 2018covering the prior calendar year 2017
Name of Signatory: Jason Chu
Title of Signatory: Manager of Information Security

I, Jason Chu, certify that I am an officer of New Century InfoComm Tech. Co. Ltd., and acting as an agent of Company, that I have personal knowledge that 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 Company's procedures ensure the company is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the Commission's rules.

Company has not taken any actions (instituted proceedings or filed petitions at either state commissions, courts, or at the FCC) against data brokers in the past year. Company has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (*e.g.,* through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps the company has taken to protect CPNI include updating its CPNI practices and procedures and conducting new training designed to ensure compliance with the FCC's modified CPNI rules.

Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Jason Chu

Manager of Information Security Department
New Century InfoComm Tech. Co. Ltd.

Date: 2018.3.1

Customer Proprietary Network Information Certification
Attachment A

Company has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures, which have been updated so that they are adequate to ensure compliance with the Commission's CPNI rules, as modified by the Commission in 2007.

Safeguarding against pretexting

- Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. Company is committed to notify the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and data brokers.

Training and discipline

- Company trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out the Company's obligation to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for marketing campaigns.

- Company employees are required to review Company's CPNI practices and procedures set forth in our current CPNI policy and training materials and to acknowledge their comprehension thereof.

- Company also requires all outside, billing contractors, to review Company's CPNI practices and procedures and to acknowledge receipt and review thereof.

- Company has an express disciplinary process in place for violation of the company's CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

Company's use of CPNI

- Company 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 subscribers 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 out-out, as applicable.*

- Company does not disclose or permit access to CPNI to track customers that call competing service providers.

- Company discloses and permits access to CPNI where required by law (*e.g.*, under a lawfully issued subpoena).

Customer approval and informed consent

- Company has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.

  - Prior to any solicitation for customer approval, Company notifies customers of their right to restrict the use of, disclosure of, and access to their CPNI.
  - Company uses opt-in approval when using or disclosing CPNI for purposes other than permitted under opt-out approval or in 47 USC 222 and the FCC's CPNI 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 year.
  - Company provides individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.
  - The content of Company's CPNI notices complies with FCC rule 64.2008(c).

  Opt-out

  - The Company currently does not use opt-out approval but reserves the right to use such procedures where permitted by law and will comply with all Commission rules regarding the use of opt-put procedures.

  Opt-in

  - Company uses opt-in approval for marketing by independent contractors and joint venture partners and for the marketing of non-communications related services by itself and its affiliates. When Company uses opt-in approval, Company provides notification consistent with FCC rule 64.2008(c).

  One time use

  - After authentication, Company uses oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice comports with FCC rule 64.2008(f).

Additional safeguards

- Company maintains for at least one year records of all marketing campaigns that use its customers' CPNI, including a description of each campaign and the CPNI used, the products offered as part of the campaign, and instances where CPNI was disclosed to third parties or where third parties were allowed access to CPNI. Such campaigns are subject to a supervisory approval and compliance review process, the records of which also are maintained for a minimum of one year.

- Company has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules for outbound marketing situations and maintenance of records.

- Company designates one or more officers, as an agent or agents of the company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC rule 64.2009(e).

- Company will provide written notice to the Commission in accordance with the requirements of FCC rule 64.2009(f) if ever its opt-out mechanisms malfunction in the manner described therein.

- For customer-initiated telephone inquiries regarding or requiring access to CPNI, Company authenticates the customer (or its authorized representative), through a pre-established password, without prompting through the use of readily available biographical or account information. If the customer cannot provide a password, then Company only discloses call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record.

- For online customer access to CPNI, Company authenticates the customer (or its authorized representative) without the use of readily available biographical or account information. After the customer has been authenticated, Company utilizes a customer-established password to authorize account access. Company establishes passwords and has employed back-up authentication for lost or forgotten passwords consistent with the requirements of FCC rule 64.2010(e).

- Company discloses CPNI to customers at Company's retail locations if the customer first presents a valid photo ID matching the customer's account information.

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

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

- In the event of a breach of CPNI, Company will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs Company to delay notification, or Company and the investigatory party agree to an earlier notification. Company will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.

- When Company discloses to or provides independent contractors or joint venture partners with access to CPNI, it does so pursuant to confidentiality agreements that (a) require the independent contractor/joint venture partner to use CPNI only for the purpose it has been provided, (b) prohibit independent contractor/joint venture partners' disclosure of such CPNI except under force of law, and (c) require the independent contractor/joint venture partner to have appropriate protections in place to ensure the ongoing confidentiality of the CPNI.