Annual Customer Proprietary Network Information Certification
Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36
January 25, 2018

Annual 64.2009(e) CPNI Certification for Calendar Year 2018

Company: NobelBiz, Inc.

499 Filer ID: 827076

Name of Signatory: Colleen Guffey

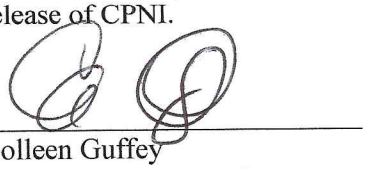
Title: Chief Compliance Officer

I, Colleen Guffey, certify that I am an officer of NobelBiz, Inc. ("Company"), 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 file petitions at either state commissions, courts, or at the FCC) against any 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.

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



Colleen Guffey
Chief Compliance Officer
NobelBiz, Inc.

Date: _01/25/2018_____

Customer Proprietary Network Information Certification
Attachment A

NobelBiz, Inc. ("Company") has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, an amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in section 64.2001 – 64.2018 of the Commission's rules. This attachment summarizes those practices and procedures.

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 notifying the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and date 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) understands what CPNI is, (b) join in and carry-out Company's obligations to protect CPNI, and (c) understand when they are and when they are not authorized to disclose CPNI.

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

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 or, 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 addition services to customers that are within the same categories of service to which the customer already subscribes.
    - To market services formally 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, as applicable.*

- Company does not disclose or permit access to CPNI to trace 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 does not use CPNI for any purpose that requires prior customer approval. For example, Company does not use CPNI to market additional services to customers that are not within the same categories of service to which the subscriber already subscribes. If this policy changes, Company will institute policies and procedures to ensure that its use of CPNI is in compliance with the FCC's regulations, including obtaining prior customer approval to use CPNI and keeping a record of all marketing campaigns that use CPNI.

Additional Safeguards

- Company has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules.

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

- Company does not provide call detail information over the phone based on customer-initiated inquiries. Company will only provide detail information by calling the customer at the telephone number of record or by sending the information to the address of record.

- In the event of a breach of CPNI, Company will notify law enforcement as soon as practicable as and no later than seven (7) business days from discovering the breach. Affected 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 modification sent to law enforcement and affected customers.