

KELLEY DRYE & WARREN LLP

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400

3050 K STREET, NW

WASHINGTON, D.C. 20007-5108

(202) 342-8400

NEW YORK, NY

CHICAGO, IL

STAMFORD, CT

PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES

MUMBAI, INDIA

FACSIMILE

(202) 342-8451

www.kelleydrye.com

DIRECT LINE: (202) 342-8640

EMAIL: dcrock@kelleydrye.com

March 2, 2009

VIA ECFS

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

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

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), NobelTel, LLC and NobelBiz, Inc. hereby
provide their Annual Customer Proprietary Network Information Compliance Certification.
Please feel free to contact me if you have any questions regarding this filing.

Sincerely,



Devin L. Crock

Annual Customer Proprietary Network Information Certification
Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36
February 27, 2009

Annual 64.2009(e) CPNI Certification for Calendar Year 2008

Company: NobelBiz, Inc.
499 Filer ID: 827076
Name of Signatory: Richard L. Mahfouz
Title: President

I, Richard L. Mahfouz, 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 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.

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


Richard L. Mahfouz
President
NobelBiz, Inc.

Date: 2-27-09

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, 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.

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 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 Company's obligation to protect CPNI, and (c) understand when they are and when they are not authorized to use or 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 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 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 compliance 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 call 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 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.

Annual Customer Proprietary Network Information Certification
Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36
February 27, 2009

Annual 64.2009(e) CPNI Certification for Calendar Year 2008

Company: NobelTel, LLC
499 Filer ID: 823026
Name of Signatory: Richard L. Mahfouz
Title: President

I, Richard L. Mahfouz, certify that I am an officer of NobelTel, LLC ("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 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.

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



Richard L. Mahfouz
President
NobelTel, LLC

Date: 2-27-09

Customer Proprietary Network Information Certification Attachment A

NobelTel, LLC ("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.

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 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 Company's obligation to protect CPNI, and (c) understand when they are and when they are not authorized to use or 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 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 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 compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC rule 64.2009(e).
- 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, customers must utilize a pre-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 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.