STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

Case 98-M-1343	**In the Matter of Retail Access Business Rules**
PSC – 10-09-00013-P **Consideration of Utilities' Compliance Filings**	**Utilities' Compliance Filings** **December 22, 2006**

COMMENTS OF THE NEW YORK STATE CONSUMER PROTECTION BOARD REGARDING CONSIDERATION OF UTILITIES COMPLIANCE FILINGS

Mindy A. Bockstein
Chairperson and Executive Director

Tariq Niazi
Acting Director of Utility Intervention

John Walters
Utility Intervenor Attorney

Dated: April 27, 2009
Albany, New York

NEW YORK STATE CONSUMER PROTECTION BOARD
5 EMPIRE STATE PLAZA
SUITE 2101
ALBANY, NEW YORK 12223-1556
http://www.nysconsumer.gov

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

Case 98-M-1343	**In the Matter of Retail Access Business Rules**
PSC – 10-09-00013-P Consideration of Utilities' Compliance Filings	**Utilities' Compliance Filings December 22, 2006**

COMMENTS OF THE NEW YORK STATE CONSUMER PROTECTION BOARD REGARDING CONSIDERATION OF UTILITES' COMPLIANCE FILINGS

Pursuant to a notice published in the March 11, 2009 New York State Register ("Register") and the comment period set forth in the New York State Administrative Procedures Act ("SAPA"), please accept these comments of the New York State Consumer Protection Board ("CPB") regarding the proposed plans filed by the distribution utilities to "provide customers with secure, real-time remote access to their own distribution utility account number" which the customer could voluntarily submit to an ESCO for a review of the customer's account. The CPB has grave concerns about the use of Social Security numbers as the sole or primary customer authentication in these plans.

Background

In a November 7, 2006 Order, the New York State Public Service Commission ("Commission") in Case 98-M-1343[1] denied, inter alia, Accent Energy's August 18, 2005 petition requesting that the Uniform Business Practices ("UBP") be amended to allow ESCOs to obtain directly from the distribution utilities customer account numbers on a

[1] See Case 98-M-1343 In the Matter of Retail Access Business Rules Petition of Access Energy LLC, Order Denying Petition and Making Other Findings, (issued November 7, 2006).

real-time basis. The Commission also ordered Consolidated Edison Company of New York, Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric, New York State Electric & Gas Corporation, Rochester Gas & Electric Corporation, National Grid, Keyspan Energy Delivery of New York, and Keyspan Energy Delivery of Long Island (collectively the "utilities") to submit within 45 days plans ("plans"), to provide customers with secure, real-time remote access to their own distribution utility account number, or point-of-delivery identification number used to sign up customers with an ESCO. The Commission ordered the utilities to also include in their plan filings: (1) itemized cost estimates and a timetable for implementation; and, (2) an explanation of how the proposed plan would maintain the privacy and security of customer information. All the utilities filed their plans by December 22, 2006. The Commission took no formal action on these filings until March 11, 2009, at which time a Notice of Proposed Rule Making was issued in the New York State Register inviting parties to file comments relating to the compliance plans as well as all other matters related to those filings.

CPB Position

Under Governor Paterson, information privacy, and the protection of a consumer's personal information in the marketplace are critical issues for the CPB. Pursuant to a new law that went into effect in January 2009, the CPB launched a new Identity Theft Prevention and Mitigation Program ("Program"). The Program is designed to provide resources to help New Yorkers prevent identity theft and aid victims in coping with the consequences of this crime.

According to the 2008 year-end summary of the Federal Trade Commission ("FTC"), identity theft remains the top consumer complaint nationwide.[2] Further, New York State ranks 6th per capita in identity theft complaints. The nexus between the indiscriminate use of Social Security numbers and identity theft risk has been identified in numerous reports. In its recent December 2008 report "Security in Numbers: SSNs and Identity Theft", the FTC argued against the use of Social Security numbers as the sole mechanism for customer authentication, as a matter of policy.[3]

The CPB endorses the FTC's concern and calls the Commission's attention to the "New York Social Security Protection Act" ("N.Y. Social Security Number Protection Act")[4] which became effective on January 1, 2008, more than a year after the submission date of the plans submitted in this case. This law prohibits among other things:

- Requiring a customer to transmit his/her Social Security number over the Internet, unless the connection is secure or the number is encrypted.
- Requiring a customer to use his/her Social Security number to access an Internet website unless a password, PIN or other type of authenticating device is also required for the individual to access the website.

Implicit in the New York law is a policy that Social Security numbers require a higher level of protection and that their use must be accompanied by at least one other identifier (password, PIN, etc.) which is non-public in nature. The CPB supports the consistent application of this policy not just to the Internet but also to Interactive Voice Recognition communications as well.

---

[2]See Federal Trade Commission ("FTC") Publication "Consumer Sentinel Network Data Book for January-December 2008". Also, see FTC press release dated February 26, 2009, FTC Release List of Top Consumer Complaints.

[3] See Federal Trade Commission Report, "Security in Numbers – SSNs and ID Theft", p. 4-5, issued December 2008.

[4] New York State Gen. Bus. Law §399-dd (2009)

It is the CPB's position that each of the proposed plans by the distribution utilities should be reviewed according to three (3) tests:

1. Does the plan rely on the use of a Social Security number as the sole authentication element?

2. If "no", is the additional authentication element non-public in nature (e.g., a PIN, not a zip code)?

3. If access is provided through the Internet, is the connection secure (e.g., https) or is the Social Security number encrypted?

After applying this review, we believe that the Commission will concur with the CPB that each of these plans raise grave security and privacy concerns requiring rejection and further modification.

Utility Proposed Plans

The proposed plans of Central Hudson, Orange and Rockland, and NYSEG/RG&E all rely solely on a full or partial Social Security number as the sole authentication element. These plans do not meet the first requirement. The CPB believes that each of these plans should be rejected in their current form.

The proposed plans of Niagara Mohawk, Con Edison and Keyspan New York and Long Island, require a zip code as an additional authentication element. Because a zip code is public and readily available, these plans should be rejected in their current form. These plans do not meet the second requirement. Additionally, the proposed plan of National Fuel Gas which identifies only unspecified "non-public identifiers" fails to provide sufficient detail to assure that consumer privacy and security will be maintained and therefore should be rejected.

The CPB particularly objects to Keyspan's Internet access plan as it may be in violation of the NY Social Security Protection Act. Internet connections, particularly wireless common at "kiosks and fairs", which the November 2006 order envisioned, can

easily be hijacked by unscrupulous identity thieves. This plan does not meet the third requirement. Sensitive information contained in transmissions via this method can readily be accessed; leading to adverse ramifications for those whose information has been compromised. Unfortunately, instances of rogue employees utilizing confidential identifying information for illicit purposes have become more prevalent.[5]

Additionally, the CPB also recommends that all utilities that currently use individual Social Security numbers for any aspect of their operations be particularly cognizant that the procedures and practices they are employing in gathering and maintaining this data are sufficient to ensure compliance with both legal requirements and best information privacy practices.

Finally, the CPB also recommends that any associated costs with the implementation of new so-called remote customer access systems should be borne by the ESCOs, that benefit from these changes.

[5] See Washington Post, December 11, 2008 Pair Charged in Identity Theft Scheme In Similar, Separate Case, D.C. Schools Employee, Friend Sentenced to 6 Months. P. BO – 2. Describing a case in which an employee of the Library of Congress, a US government employee, was charged with stealing the identities of ten individuals via the utilization of stolen social security numbers.

Conclusion

For the reasons stated above, the CPB recommends that all of the proposed plans be rejected in their current form. Further, if any utility is engaged in a practice which violates the New York Social Security Protection Act, the Commission should order such practice to cease immediately. The CPB stands ready to assist the PSC to advance the privacy of customers.

Respectfully submitted,

Mindy A. Bockstein
Chairperson and Executive Director

Tariq Niazi
Acting Director of Utility Intervention

John Walters
Intervenor Attorney

Dated: April 27, 2009