

STATE OF NEW YORK

Public Service Commission

Garry A. Brown, Chairman

Three Empire State Plaza, Albany, NY 12223

Further Details: James Denn

James.Denn@dps.ny.gov | 518.474.7080

<http://www.dps.ny.gov>

<http://twitter.com/NYS DPS>

12059/12-M-0282

PSC TELLS NYSEG, RG&E TO IMPROVE CONSUMER SAFEGUARDS — Investigation into Security Breach of Consumer Information Spurs Call for Change —

Albany, NY—7/12/12—The New York State Public Service Commission (Commission) today received a report from Department of Public Service staff that both New York State Electric & Gas Corporation (NYSEG) and Rochester Gas & Electric (RG&E) failed to adequately protect confidential customer information from unauthorized access by outside parties.

“Our investigation found that NYSEG and RG&E failed to meet industry standards and best practices to protect personally identifiable information of customers,” said Commission Chairman Garry Brown. “As a result, we are directing the companies to immediately take action to address the vulnerabilities on its computer billing and records systems currently used to take and maintain confidential customer information.”

In January 2012, NYSEG advised the Department that unauthorized parties had obtained access to confidential information of both NYSEG and RG&E customers, including Social Security Numbers, dates of birth, and in some cases, financial institution account information.

The Department immediately commenced a review of actions taken by NYSEG/RG&E to inform and assist their customers, including efforts to provide accurate information about the potential impact of this security breach and to provide tools to assist customers in identifying instances in which their confidential information was misused. The Department also began an investigation to identify deficiencies in NYSEG/RG&E systems and procedures regarding the protection of

confidential customer information, including those that may have contributed to the incident, and to develop recommendations for corrective action.

According to the report's findings, there is no evidence to date that any confidential customer information was misused. After the companies became aware of the security breach, they generally took reasonable actions to inform their customers of the potential impact of the breach. However, several deficiencies in the companies' systems and practices contributed to the security breach. Since then, the companies' have taken sufficient steps to prevent a recurrence of a similar security breach and the companies are planning a major revamp of the information systems and data protection security.

Based upon the investigation's findings, the companies should further refine policies, processes and procedures regarding confidentiality safeguards. The companies should minimize access to the most sensitive personally identifiable information by maintaining a strictly "need to know" standard for contractors and employees alike. The companies should conduct, at least annually, an incident response exercise simulating a breach of such data. The companies should establish a protocol for notification of regulators in the event of any significant cyber incident involving a possible compromise of customer data; and the companies should promptly implement steps to ensure the security of all data stored on company mobile computers and removable data storage media.

The companies are to report within 60 days of the order on progress in implementing the recommendations, and to include in such report the companies' plans for handling the costs incurred in responding to this breach and how such plan complies with the companies' respective rate plans.

In addition to the foregoing recommendations, the Commission raised concerns that the issue of costs that both the companies incur in responding to this security breach. The Commission will require the companies segregate and report all of the costs associated with rectifying the security breach, including the customer care costs identified above as well as any incremental investigation and remediation costs, as part of respective 2012 earnings sharing filings, and that

the Commission closely scrutinize any proposal to incorporate these costs in the earnings sharing calculation. In this way, the companies will be put on notice that they will be required to justify fully the inclusion of any such expenses in their earnings sharing calculations.

Although NYSEG and RG&E have made strides toward safeguarding data, the Commission seeks to share lessons learned with all of the larger utilities. As a result, the Commission will require further efforts to ensure that all large utilities remain focused on these issues and have procedures to protect personally identifiable customer information. The Commission will therefore direct large utilities to provide the status of their implementation of best practices for the protection of personally identifiable information.

The staff report today, when issued, may be obtained by going to the Commission Documents section of the Commission's Web site at www.dps.ny.gov and entering Case Number 12-M-0282 in the input box labeled "Search for Case/Matter Number". Many libraries offer free Internet access. Commission orders may also be obtained from the Commission's Files Office, 14th floor, Three Empire State Plaza, Albany, NY 12223 (518-474-2500).