STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on August 15, 2013

COMMISSIONERS PRESENT:

Garry A. Brown, Chairman
Patricia L. Acampora
Gregg C. Sayre
Diane X. Burman

CASE 13-M-0178 - In the Matter of a Comprehensive Review of Security for the Protection of Personally Identifiable Customer Information. Review of Central Hudson Gas and Electric Corporation Breach Incident.

ORDER DIRECTING THE CREATION OF AN IMPLEMENTATION PLAN

(Issued and Effective August 19, 2013)

BY THE COMMISSION:

BACKGROUND

On February 16, 2013 Information Technology (IT) personnel at Central Hudson Gas and Electric Corporation (Central Hudson) discovered anomalous activity on the company's business systems computer network. The activity indicated that malicious software may have been introduced, possibly resulting in a breach of company network security. Monitoring of this activity revealed that a company desktop computer connected to a cash and check processing system for customer bill payment management was attempting to log onto other Central Hudson network systems using local accounts.

Over the next three days investigation by company IT employees determined that malware had in fact made its way into the company network and that the malware had disabled antivirus software on a company desktop computer. Central Hudson immediately identified all internet addresses that could be

associated with the anomalous traffic and blocked those addresses in an effort to contain the problem. On February 19, 2013, Central Hudson's president informed Chairman Brown of the breach and a company vice president notified Utility Security Section staff (Staff) of the Department of Public Service (Department).

INVESTIGATION by DELL SECUREWORKS

Central Hudson secured the services of Dell SecureWorks (Dell) to investigate the incident. Dell conducted an on-site investigation commencing on February 19, 2013.[1]

Dell concluded from its investigation that the malicious software was of a type popularly known as a "worm". This particular malware has the capability of avoiding detection of its presence by disabling antivirus and malware detection software and spreading itself over an organization's network. It even has the ability to update itself as it is gathering information and securing persistent illegal remote access to a computer. This worm was designed to steal user information, and then look for avenues by which to send the information it has found, out of the company network. This malware typically infects networks by lurking on legitimate websites and through the hacking technique of phishing (sending e-mails soliciting a user click). With this design capability, the malware found by Dell in the Central Hudson network is an ideal identity theft tool.

Dell was unable to conclusively determine when or how the malware gained entry to the Central Hudson network. Dell

[1] Central Hudson also notified the New York State Police. Forensic information gathered by Dell was shared with the State Police.

did confirm that the malware had been present within the Central Hudson network at least six months prior to the discovery and possibly earlier. Dell was not able to determine from its forensic analysis precisely when or by whom the malware was introduced. Nor has it been possible to determine the quantity and the content of the data that may have been transferred out of Central Hudson's control during the file transfer connections that were self-initiated by the worm. Due to the fact that the malware is known to have infected a company system that processes customer payment made by personal check, together with scans and other records of the information printed on the check, the personally identifiable information (PII) found on the face of those checks had to be considered compromised.

CENTRAL HUDSON RESPONSE TO CUSTOMERS

On February 22, 2013, Central Hudson began to notify customers of the incident by issuing press releases, posting information on its website and making outbound automatic phone calls. Additionally, the Company sent two sets of mailings to the approximately 110,000 potentially affected residential and non-residential customers to provide information about the breach, how customers may be affected and the actions that customers should take to determine if their confidential information has been misused. The Department's Office of Consumer Policy reviewed the second set of correspondence and recommended modifications to stress the importance of the message and to clarify that free credit monitoring services were available for a limited time.

The Company announced that it was offering its customers the option of one year of credit monitoring service from Experian, one of the nation's largest credit reporting entities, at no charge. Central Hudson announced that its

customers must enroll in the Experian program by June 30, 2013. The Experian service provides customers with a copy of their credit report, daily monitoring and alerts regarding suspicious activity, and an insurance policy to help cover certain costs in the event that customer identity theft occurs. Central Hudson indicated that it will record costs incurred as operating expenses and will not be requesting separate reimbursement or deferral of such costs for future recovery from customers.

The Department requested and received weekly reports containing the number of Central Hudson customers who enrolled in the free credit monitoring service. As of July 7, 2013, 21,405 residential and 1,094 non-residential customers have enrolled in the service. Central Hudson also said that it will provide Staff with immediate notice of any findings by Experian or law enforcement entities that relate to this incident. Central Hudson reports, however, that it has no information indicating that there has been any inappropriate use of customer data attributable to this incident so far.

DELL'S RECOMMENDATIONS TO CENTRAL HUDSON

Dell provided several recommendations to Central Hudson to lessen the possibility of a future breach of company network security from malicious software introduced via the internet. Those recommendations included more frequent changing of employee passwords, rigorous password policy enforcement, frequent antivirus software updates, frequent software security updates of operating system and third-party software, resetting Internet browser settings to make them more restrictive, more frequent inventory and destruction of stored customer

information, and further limiting of removable storage media in the workplace.[2]

Dell also emphasized the importance of regular and frequent employee cyber security awareness training, particularly with regard to the increasingly more sophisticated phishing techniques designed to lure unsuspecting employees to innocent appearing web links that are in fact malicious.[3] In addition, Dell offered recommendations for the deployment of less conventional and more comprehensive technical cyber security measures. These measures would allow only use of preapproved software applications recognized and known to be safe, and to block inbound and outbound network traffic on the company network that did not conform to preset specifically configured traffic types. These more advanced technical protective steps included "White Listing" (a default setting that limits employee access to software applications known to be safe and only to internet traffic that meets certain preset security rules) and the deployment of a Data Loss Prevention (DLP) system solution.

Staff met with Central Hudson executives and IT management, along with representatives from Dell SecureWorks to examine the full Dell report. Staff discussed the findings and recommendations included in the report with Central Hudson personnel and with the Dell representatives, along with

[2] Portable storage media, such as thumb drives, can be the source of accidental and deliberate malware infections when plugged into a network machine.

[3] These recommendations, as well as others that Dell made could be considered basic cyber security measures and were already part of Central Hudson's cyber security program. Dell urged more frequent and rigorous application of such measures.

projected timetables and various means by which Central Hudson would act on the Dell recommendations.

In summary, Dell Secureworks submitted 13 recommendations to Central Hudson. Of those:

- 6 have been adopted and fully implemented.
- 3 have been partially implemented, with full implementation targeted for 2014
- 4 are under review, with company projected determinations for action or implementation, by late 2013 or 2014.

CONCLUSION

Central Hudson is directed to develop an Implementation Plan (the Plan) within 30 days of the issuance of this Order to be maintained at the Company's premises and made available to Department Staff upon request for review and inspection. The Plan should include all actions taken, or planned to be taken, in response to the recommendations submitted to the Company by Dell SecureWorks in March 2013. The Plan should include an overall assessment of the relative priorities for each of the recommendations, implementation action steps taken or yet to be taken, proposed alternative measures, schedules with specific interim milestones, and any Dell recommendations rejected by Central Hudson with a comprehensive explanation as to why such were rejected. If Central Hudson believes a recommendation should not be implemented, full justification supporting the Company's determination should be provided.

Central Hudson should consult with Staff during the development of this plan.

The Commission orders:

1. Central Hudson is directed to create an implementation plan within 30 days of the issuance of this Order

consistent with the procedures and requirements detailed in the body of this Order.

2. This proceeding is continued.

By the Commission,

Kathleen H. Burgess

Digitally Signed by Secretary
New York Public Service Commission

KATHLEEN H. BURGESS
Secretary