COMMISSIONERS
JEFF HATCH-MILLER - Chairman
WILLIAM A. MUNDELL
MARC SPITZER
MIKE GLEASON
KRISTIN K. MAYES

BRIAN C. MCNEIL
Executive Secretary

ARIZONA CORPORATION COMMISSION

June 27, 2005

Mr. James S. Pignatelli
President and CEO
UniSource Energy Corporation
Post Office Box 711
Tucson, AZ 85702

VIA FACSIMILE

Re: Utility Customer Data Security
Docket No. ACC-00000A-05-0453

Dear Mr. Pignatelli:

Identity theft, data mining, "phishing" and virus infection are huge and growing problems in this country. They are problems about which every consumer, including utility customers, has a right to be concerned. As a wired and interconnected society, we are always vulnerable to cyberthiefs. Sensitive data about our personal and professional lives can, and does, find its way into the wrong hands.

Household names like CVS and Kaiser Permanente recently settled with federal regulators over data security breaches. Every major news outlet has carried the recent story of CardSystems Solutions, a Tucson company that processes transactions for MasterCard and Visa. As many as 40 million credit card accounts may be compromised because of lax safeguards or weaknesses in the security infrastructure.

As you know, utility customers are increasingly opting to pay bills online. Beyond that, utility company databases contain the kind of information that a skillful hacker might seek to exploit for financial gain or wreak havoc for pure sport. I am writing to you today to gather information on the measures your company is undertaking to ensure data security for your customers. Specifically, I am requesting your written responses to the following questions. I have asked that an informational docket be opened to gather and review these responses. Please submit your responses to Docket Control by July 25, 2005.

General Questions

1 What steps do you take to safeguard your customers' data from hacker attempts?
2 Does your Information Technology system employ intrusion detection and prevention measures, anti-virus defenses, and firewalls?
3 If a large-scale attempt to steal customer information were successful, does the utility have an obligation to notify the Federal Trade Commission or other federal regulatory body (in addition to notifying the Commission)?

4 How many attempts to hack into your databases are thwarted by your security measures? (Please indicate whether these are daily, weekly or monthly figures.)
5 What kind of on-going training does your technology staff undergo to keep current on the latest advances in software security?

Utility Relationships with Off-Site Vendors

1 Many utilities maintain relationships with outside vendors for billing, sales or collections efforts. To the extent that this is true for your Arizona operations, please indicate the names of your vendors, the services provided by the vendors and the general details of the vendor-utility information sharing.
2 How frequently do you audit vendors to ensure utmost security of customer data?
3 Are independent security auditors used by your utility? If so, how frequently?

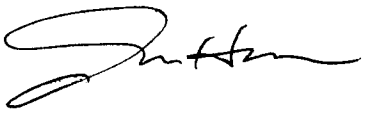
Internal Security

1 What safeguards do you take to ensure that your employees do not gather or use sensitive or identifying customer information?
2 Do you have an identity theft/data security policy to which staff members must adhere? Please provide a copy of any such policies to the Commission.
3 If an employee violates these policies, what steps do you take to notify customers of the problem and what consequences does the employee face?

I realize that any interconnected, computerized system cannot be 100% secure at all times. I invite you to provide any additional data that would help reassure me that your utility is safeguarding customer data to the fullest extent possible.

Thank you for your cooperation in this matter.

Sincerely,



Jeff Hatch-Miller
Chairman

CC: Commissioner William A. Mundell
Commissioner Marc Spitzer
Commissioner Mike Gleason
Commissioner Kristin Mayes
Brian C. McNeil
Heather Murphy
Ernest Johnson
Chris Kempley
Lyn Farmer