

**STATE OF ILLINOIS
ILLINOIS COMMERCE COMMISSION**

Illinois Commerce Commission)	
On Its Own Motion)	
Investigation into the Customer)	Docket No. 15-0073
Authorization Required for Access by Third)	(January 28, 2015)
Parties Other than Retail Electric Suppliers)	
To Advanced Metering Infrastructure Interval)	
Meter Data)	

VERIFIED COMMENTS OF THE MISSION:DATA COALITION

The Mission:data Coalition¹, a national coalition of technology companies delivering data-enabled consumer-focused energy services and solutions², appreciates the opportunity to provide these Verified Comments in the Investigation into the Commission investigation addressing “Customer Authorization Required for Access by Third Parties Other Than Retail Electric Suppliers to Advanced Metering Infrastructure Interval Meter Data.”

In ICC Docket 15-0073, the Illinois Commerce Commission (“Commission” or “ICC”) “seeks to investigate the need for, and form of, customer authorization required for access by third parties, other than Retail Electric Suppliers (‘RES’), to Advanced Metering Infrastructure (‘AMI’) interval meter data.” Following a workshop held on February 3, 2015 concerning these matters, Citizens Utility Board (“CUB”) circulated a proposed common outline for the first round of verified comments. We have used that outline to organize our remarks.

¹ www.missiondata.org

² Our members are developing innovative information technologies to achieve significant energy savings in both the residential and commercial sectors at scale. They include Alarm.com, Bidgely, BlueLine Innovations, BrightPower, BuildingIQ, the Cleanweb Initiative, EcoFactor, EnerNOC, EnergyHub, FS Energy, Genability, Home Energy Analytics, iControl Networks, kW Engineering, Lucid, People Power, Plotwatt, Rainforest Automation, Retroficiency, Solar City, Stem, ThinkEco, Verdafero, Switchornot.com, Utilisave and WattzOn.

I. The Need for Commission Direction on Customer Authorization

To fully realize the benefits of AMI, customers must have the ability to easily and rapidly authorize the sharing of their electricity usage information with third-party energy services of their choice, especially those that are not retail suppliers. In the Initiating Order, the Commission expresses its desire to investigate the need for, and the form of, customer authorization required for access by third parties to customer's smart meter information. In order to ensure that consumers have access to the full energy-saving benefits made possible by Illinois' advanced metering infrastructure in a way that protects their confidential energy usage information, we believe it is appropriate for the Commission to establish standard language and clear rules so that consumers remain confident in the process and the services being offered.

II. Guiding Principles

Mission:data believes consumers should have convenient electronic access to the best available information about their own electricity use in order to fully leverage consumer benefits made possible by AMI. Our goals match Section 16-108(d) of the Public Utilities Act ("PUA"), namely: "[to] establish the right of consumers to consent to the disclosure of personal energy information to third parties through electronic, web-based, and other means..." By establishing standard service guidelines under which utilities must accept a customer's authorization to share usage data with a third party, the Open Data Access Framework will establish Illinois as a leader in empowering its consumers with the means to better manage their energy use. Mission:data, which has engaged on behalf of consumer data access before public service commissions across the country, is pleased to join leading consumer and environmental organizations in strong support of the Open Data Access Framework.

We recognize that authorization processes for Retail Energy Suppliers ("RESs") have been considered in Docket No. 13-0506. Of particular note was the Commission's determination that "verifiable authorization," per Section 16-122(a) of the PUA, is required for interval meter data, whereas only a customer account number was sufficient to authorize monthly usage data to RESs. We recognize

this precedent, and thus we believe it is the Commission’s intention to more clearly define “verifiable authorization” for non-RES third parties in this proceeding, since interval meter data, not monthly bill data, is in question. Toward that end, we propose the following Guiding Principles that we believe will simultaneously define acceptable “verifiable authorization” processes and support the larger goal of a robust market for innovation that will bring new services with direct benefits to consumers:

- **Simplicity:** Customer authorization language *and* authorization processes should be clear, simple and support a customer’s general understanding of the authorization they are providing. The required process should feature clear and streamlined customer authorization language that can be implemented quickly and easily by the utilities and third parties while ensuring appropriate disclosures are given to customers.
- **Convenience:** Customers should be able to provide authorization in a manner that is convenient and consistent with the common practices in other areas of their digital lives. Therefore, customer authorization processes should support multiple methods for providing service providers access to their information. Any authorization language and processes should anticipate not just traditional paper and electronic processes, but evolving web-based applications and mobile technology, such as user authentication by text messages.
- **Direct:** Customers should be able to provide authorization through simple “one-stop shopping” formats. That is, consumers should be able to provide authorization directly to their preferred service providers through forms, web sites and mobile applications available from those third parties. Any process approved should involve the fewest steps necessary by a customer. To ensure non-discrimination, utilities should limit the users’ inputs on web or mobile applications to *only* what is required to authenticate the user, authorize the third party and comply with Commission rules. It should not require that access to the data just rest with one party such that a potential client has to give up their direct access to the data so as to enable a service provider to gain such access; rather a customer should be empowered to grant access to multiple service providers of his or her choice.

- **Verification by Utilities:** Any authorization process should avoid placing the utility in the position of reviewing or policing third-party requests for usage data on any criteria except those which are deemed absolutely necessary for third parties to register with the utilities. (For examples of other states' third party registration processes with utilities, see Mission:data's Nov 6th, 2014 Response to ICC Commissioners Data Request in Docket No. 14-0507.) To the greatest degree possible, utilities should be released from liability arising from potential misrepresentation, abuse or misconduct by third parties.

If these guiding principles of the authorization process are heeded, then the Open Data Access Framework -- which commands broad support among organizations representing consumers, environmentalists, technology companies and others desiring consumer-enabled energy innovation -- will be poised to accomplish its objectives as well as satisfy Section 16-108.6(d) of the PUA.

III. Authorization Language

We believe that consistent language will support consumer confidence, ease of use and customer-friendly implementation. A recognized best practice in privacy and security is for disclosures to consumers to coincide with the consumer's choice – for example, software license agreements that require acceptance immediately prior to installation, or push notifications that accompany application downloads. Third parties should apprise customers of critical facts such as the term of the authorization and their right to terminate, but the authorization language should be short and to the point so that customer disclosures and authorizations can be legible on mobile devices.

Consistent with the above characteristics of ease of use and brevity, we find the proposed language from CUB acceptable:

"I, [CUSTOMER NAME] authorize [UTILITY] to provide my electricity usage information ("EUI") to [NAME OF THIRD PARTY]. The EUI includes my electricity usage levels for distinct time periods no longer than 60 minutes to the extent this information has been recorded and retained by [UTILITY]."

I authorize [THIRD PARTY] to access my electricity usage information for the previous 24 consecutive monthly billing cycles as well as future monthly billing cycles. This authorization to access and use my EUI will expire (a) after 24 months unless otherwise specified in the terms of service agreement with (NAME OF THIRD PARTY), (b) upon notification of the termination of service with (NAME OF THIRD PARTY), unless otherwise specified in the terms of service agreement with (NAME OF THIRD PARTY) or (c) upon notification that I have revoked (NAME OF THID PARTY)'s authorization to access my EUI.

Mission:data suggests that the term "EUI" be replaced by "electricity usage information" simply to avoid jargon. Consistent with commonly accepted privacy principles, it is appropriate to provide the consumer with an understanding of what services the authorization will be used to support, such as "the provision of energy management services." However, we do not believe that there should be restrictions on the purposes that consumers may find valuable and that may be offered in the future.

IV. Authorization Process

Mission:data believes that the Commission should proceed carefully with regard to requiring a specific authorization process. The problem with being overly specific about an authorization process in a Commission ruling is that evolving technologies might someday be able to accomplish the same outcomes in a new way, rendering Commission rules obsolete. Further, we do not believe it is the Commission's practice to micro-manage every technical detail of an authorization process, so long as it meets Commission requirements and satisfies state law. Nevertheless, there are certain standards that should be followed, and general attributes of the desired authorization process can be spelled out while the implementation details can be left to the utilities to manage.

First we will discuss a specific authorization mechanism in the Energy Services Provider Interface (ESPI) or Green Button Connect standard. Then we will discuss generic attributes of an authorization process that will meet the objectives of the Open Data Access Framework. Finally, we will address the three authorization scenarios raised in this proceeding.

ESPI uses a three-party authorization standard known as OAUTH. It is important to note that, in any authorization scheme, the authorization process (granting someone certain rights) is always preceded

by authentication, the process of establishing an authentic identity. Before a customer can approve a third party's access rights, the utility must be reasonably sure that the customer is, in fact, the customer, and not an imposter.

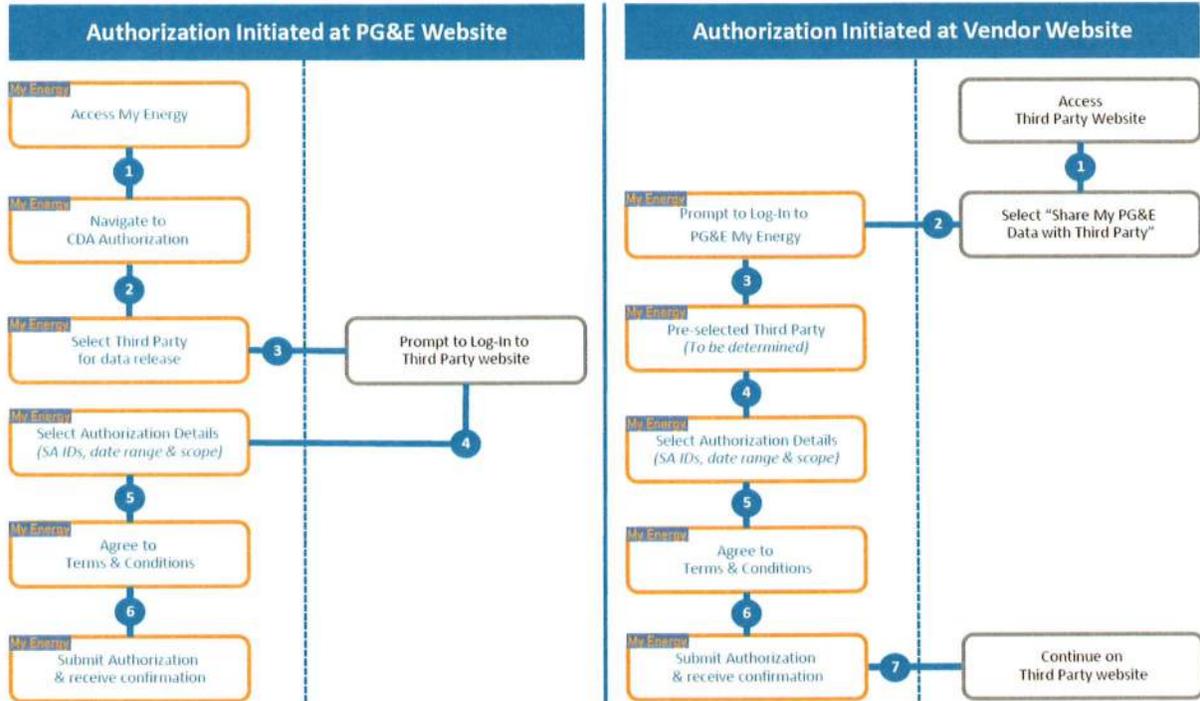
In ESPI, the authentication process occurs through the utility's website, where the user enters login credentials already established with the utility. Online accounts are usually established by a self-service website requiring the customer's utility account number, name, address, or a combination. Alternatively, an online account could be established by phoning the utility's call center and providing similar information. It is believed that unique identifiers such as the utility account number and/or address are sufficient to establish the customer's identity with reasonable certainty.

The ESPI authentication/authorization process follows one of two processes. In the first case, the customer visits the utility's website, logs in with his/her credentials, selects a third party from a list of registered companies, and clicks to authorize that third party. In the second case, the customer begins at the third party's website, logs in with his/her credentials with the third party, clicks a link that says "authorize your utility company here" (or something similar), is redirected to the utility's website to provide a login and password, and then is returned to the third party's website to complete the process. This case is similar to how Facebook, Twitter, LinkedIn and other services provide a user experience for simple authentication and authorization with third party websites. It is important to note that these two cases are equally secure – one is not inferior to the other in terms of security or authenticity. A flow diagram outlining these two cases is provided below by Pacific Gas & Electric, who recently enabled its ESPI functionality.



Online Customer Authorization

Customer may release data through one of two processes



At a minimum, the Commission should require utilities to implement both of the scenarios described above for ESPI. ESPI is standardized, and these two methods are in practice throughout the state of California today. It is reasonable to expect the same authorization process to exist in Illinois.

However, there may be other authorization processes, in addition to ESPI's, that are reasonable. An authorization on paper could still enable a third party to access usage data through ESPI, for example; web-based authorization and ESPI are not incompatible. Paper-based processes might be necessary to accommodate customers without computers, certain business customers, or others who do not have an online utility account established. One can imagine any number of authorization processes involving faxes, text messages, or emails in which customers affirm their intention of sharing usage data with a third party. What is important is not so much the medium (paper, fax, text, etc.) but rather that the

customer's identity is reasonably determined. If the utility has the customer's cell phone number on file, then texting a four-digit temporary key to the cell phone could be used to establish identity. (In that case, the customer would enter the temporary key in the third party's website, and the third party would transmit the key to the utility for validation.)

Therefore, while we encourage the Commission to require, at a minimum, the utilities to implement the ESPI authorization processes described above, we believe there are other methods that can and should be sanctioned that provide flexibility to different customers while assuring the utility that the authorization is not fraudulent. We do not believe it is the Commission's job to prescribe the technical specifics of each method. However, we strongly encourage the Commission to require the utilities to implement several flexible authorization mechanisms in order to reach all customers with whatever tools and technologies are available to them.

Scenarios

Scenario 1 – Warrant: As described above, we believe the so-called warrant should be only one of many different non-web-based authorization scenarios encouraged by the Commission.

Scenario 2 – One-time: The one-time authorization *could* be Green Button Connect – for example, in authorizing a third party from the utility's website using the ESPI process described above, the user could check a box that says "One-time only." This would be different from an on-going authorization. It is important for all parties to this proceeding to understand that the authorization process has almost nothing to do with the protocol for data transmission; they are each independent. ESPI can be authorized by a paper form or a website login or a text message. The important thing is that, regardless of ESPI, the authorization process should follow the "Guiding Principles" we specified above and accommodate various technological methods, including text messages and mobile applications.

Scenario 3 – On-going Electronic: Please see the diagram above. We believe that these two methods should, at minimum, be required. However, as argued above, it is important to leave the door open for other authorization methods to evolve in the future.

Term of Authorization

The Open Data Access Framework proposes a default term of authorization that expires after 24 months unless otherwise specified in the terms of service agreement between the customer and the authorized third party, which authorization may be renewed automatically when a customer renews his or her service contract with the third party. Mission:data discourages the use of an arbitrary limitation on the length of the authorization because of the potential to disrupt ongoing service agreements between customers and third parties, or chill innovation where business models require a longer term. The proposed language above fairly balances the concerns of the stakeholders by permitting flexibility, including the possibility of indefinite authorizations. Permitting customers to authorize third party data access without arbitrary time limitation is consistent with data access rules adopted in states like Colorado and California.³ Mission:data believes that Illinois will be similarly well-served by allowing customers and third-parties to tailor terms consistent with customer needs.

Mission:data appreciates the opportunity to submit these Verified Initial Comments and would be pleased to provide any assistance that the Commission may require. Thank you for your consideration.

Dated: March 9, 2015

Respectfully submitted,

FOR THE MISSION:DATA COALITION, INC.

_____/s/_____
Jim Hawley

_____/s/_____
Cameron Brooks

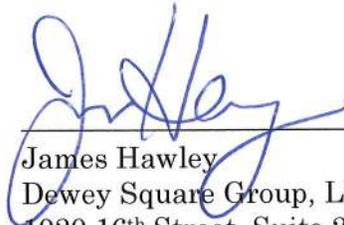
_____/s/_____
Michael Murray

³ See e.g. California Public Utilities Commission, Decision 11-07-056 July 28, 2011, p. 81.

STATE OF CALIFORNIA)
)
COUNTY OF SACRAMENTO) SS

VERIFICATION

I, James Hawley, state that I have read the foregoing Initial Comments of the Mission:data Coalition, Inc. for ICC Docket No. 15-0073, that I know the contents thereof, and that to the best of my knowledge, information, and the belief, based upon reasonable inquiry, the contents are true and correct.



James Hawley
Dewey Square Group, LLC
1020 16th Street, Suite 20
Sacramento, CA 95814
(916) 288-2228
jim.hawley@deweysquare.com

Notarized this ___th day of March, 2015.

Notary Public

**See Attached California
All-Purpose Acknowledgement**

ACKNOWLEDGMENT

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of Sacramento)

On 3-9-15 before me, Olin E. Rust, Notary Public
(insert name and title of the officer)

personally appeared James Hawley
who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/~~she~~/they executed the same in his/~~her~~/their authorized capacity(ies), and that by his/~~her~~/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature Olin Rust (Seal)

