Fleming-Mason Energy

A Touchstone Energy Cooperative

March 20, 2013

Mr. Jeff Derouen, Executive Director
Kentucky Public Service Commission
211 Sower Boulevard
P.O. Box 615
Frankfort, Kentucky 40602

RE: PSC Case 2012-00428 First Request for Information

Dear Mr. Derouen:

Enclosed for filing are an original and fourteen (14) copies of the responses of Fleming-Mason Energy Cooperative for the first request for information and the responses to the Attorney General's initial data request for the above referenced case. Please feel free to call if you have any questions or concerns.

Sincerely,

Joni Hazelrigg

Joni Hazelrigg
CFO

Enclosures

CC: Parties of Record

COMMONWEALTH OF KENTUCKY

BEFORE THE PUBLIC SERVICE COMMISSION

In re the Matter of:

CONSIDERATION OF THE IMPLEMENTATION	)	
OF SMART GRID AND SMART METER	)	CASE NO.
TECHNOLOGIES	)	2012-00428

FLEMING-MASON ENERGY COOPERATIVE, INC.'S

RESPONSES TO COMMISSION STAFF'S FIRST REQUEST FOR INFORMATION DATED FEBRUARY 27, 2013

I, Christopher S. Perry, President & CEO, of Fleming-Mason Energy Cooperative, Inc., declare that the statements contained in this response are true to the best of my information and belief.

Christopher S. Perry, President & CEO
Fleming-Mason Energy Cooperative, Inc.

Subscribed and sworn to before me by Christopher S. Perry, this 18th day of March, 2013.

Notary Public, State-At-Large

My commission expires: June 20 2014.

Request 98. With regard to calendar years 2007 through 2012, identify and discuss what Smart Grid and/or Smart Meter initiatives the utility implemented. The discussion should include but not be limited to the reasons why each initiative qualifies as a Smart Grid and/or Smart Metering initiative; the date of installation; the total cost of installation; and any benefits resulting from the initiatives, quantifiable or otherwise, received by both the utility and the customers.

Response:

Fleming-Mason Energy filed for a Certificate of Public Convenience and Necessity with the PSC on August 1, 2012 to install an Advanced Metering Infrastructure system (AMI). The PSC granted the CPCN (Case No. 2012-00361) on October 11, 2012. Fleming-Mason expects to deploy the first meters on the AMI system in August, 2013. Please reference Case No. 2012-00361 for a complete analysis of the AMI system.

Fleming-Mason has filed for a new Time-of-Day rate with the PSC (Case No. 2012-00369). This case is not yet complete but if the new rate is approved, Fleming-Mason will be able to offer customers this option to reduce peak usage as well as reduce their electric bills by shifting kWh usage to non-peak times at a reduced rate.

Request 99. With regard to calendar years 2013 through 2018, identify and discuss what additional Smart Grid and/or Smart Meter initiatives the utility has forecasted to be implemented. The discussion should include but not be limited to why each forecasted initiative qualifies as a Smart Grid and/or Smart Metering initiative; the forecasted date of installation; the forecasted total cost of installation; and any forecasted benefits to result from the initiatives, quantifiable or otherwise, received by both the utility and the customers.

Response:

Please reference the response to Request 98 and Case No. 2012-00361. Fleming-Mason's AMI deployment will begin in August, 2013 and plans to be completed in September, 2015.

Request 100. With regard to DA Smart Grid Initiatives provide the following:

a. the number of DA systems installed as of December 31, 2012, along with the associated benefits realized.

Response:

None

b. the number of DA systems to be installed in the next five years.

Response:

None planned at this time.

c. the total number of DA systems to be installed when the DA system is completely deployed.

Response:

N/A

Request 101. With regard to Volt/VAR Optimization, provide the following:

a. the number of Volt/VAR Optimization systems installed as of December 31, 2012, along with the associated benefits realized.

Response:

None

b. the number of Volt/VAR Optimization systems to be installed in the next five years, along with the forecasted in-service date.

Response:

None planned at this time.

c. the total number of Volt/VAR Optimization systems to be

installed when the Volt/VAR Optimization system is completely deployed.

Response:

N/A

Request 102. With regard to Supervisory Control and Data Acquisition ("SCADA") Smart Grid Initiatives, provide the following:

a. the number of SCADA systems installed as of December 31, 2012, along with the associated benefits realized.

Response:

Fleming-Mason is operating on an OSI SCADA platform which is owned and maintained by East Kentucky Power. Each distribution substation is equipped with data points that monitor recloser controls, voltage regulation, and metering data. Benefits include: operational control of reclosers, historical data retrieval, and fault data which aids in fault location analysis.

b. the number of SCADA systems to be installed in the next five years, along with the forecasted in service date.

Response:

No SCADA systems are schedule to be installed in the next five years.

c. the total number of SCADA systems to be installed when the SCADA system is completely deployed.

Response:

SCADA is completely installed on all twelve of FME's distribution substations.

Request 103. As it relates to Dynamic Pricing (where rates are established hourly throughout the day) Tariffs or TOU Tariffs, provide the following:

a. the number of customers the utility has or had on these types of tariffs, identified separately by specific tariff.

Response:

None

b. whether these customers shifted load from high-price times periods to lower-priced time periods.

Response:

N/A

c. whether these customers consumed more, less or the same number of kWh.

Response:

N/A

d. whether the utility reached any findings or conclusions based on its experience with customers on Dynamic Pricing and/or TOU Tariffs.

Response:

N/A

Request 104. Describe precautions taken and/or standards developed by the utility to address concerns regarding cybersecurity and privacy issues.

Response:

Fleming-Mason is working with its AMI vendor as well as its customer billing vendor to assure the highest levels of cybersecurity are utilized to protect both the utility and its customers.

Request 105. Provide a discussion and details of progress made regarding the concern raised by the utilities as it relates to the interoperability standards for Smart Grid equipment and software.

Response:

Fleming-Mason prefers software vendors to be MultiSpeak compliant and maintain IEEE Standards. MultiSpeak allows data to flow seamlessly into many applications that Fleming-Mason has in place such as the customer billing software, outage management software and load management software.

Request 106. Provide a discussion concerning how the costs (investment and operating and maintenance costs) associated with the installation of Smart Grid facilities should be recovered from the ratepayers.

Response:

Fleming-Mason references the response to PSC Request 106 submitted by EKPC and adopts that response as its own.

Request 107. State whether the utility would favor a requirement that it report to the Commission so that the Commission is aware of the jurisdictional Smart Grid and/or Smart Meter activities within the Commonwealth. As a specific example, the requirement could order that a report be provided each September regarding the Smart Grid and/or Smart Meter activities the utility is planning to perform during the upcoming calendar year, followed by an April report of the Smart Grid and/or Smart Meter activities the utility completed the preceding calendar year.

Response:

Fleming-Mason references the response to PSC Request 107 submitted by EKPC and adopts that response as its own.

Request 108. State whether the utility believes KRS 278.285 is an appropriate approach to recovering the costs (investment and operation and maintenance) associated with Smart Grid investments.

Response:

Fleming-Mason references the response to PSC Request 108 submitted by EKPC and adopts that response as its own.

Request 109. State whether the utility believes a tracking mechanism as described beginning on page 3 of the Wathen Testimony on behalf of Duke Kentucky is an appropriate approach to recovering the costs associated with Smart Grid investments.

Response:

Fleming-Mason references the response to PSC Request 109 submitted by EKPC and adopts that response as its own.

Request 110. State whether the utility has commissioned a thorough DSM and Energy Efficiency ("DSM-EE") potential study for its service territory. If the response is yes, provide the results of the study. If no, explain why not.

Response:

Fleming-Mason references the response to PSC Request 110 submitted by EKPC and adopts that response as its own.

Request 111. Refer to the Munsey Testimony on behalf of Kentucky Power, page 10, lines 11-19 regarding the Green Button initiative. Describe the extent of your utility's participation in this industry-led effort.

Response:

Upon deployment of its AMI, Fleming-Mason will be able to offer up-to-date usage data that can be viewed from a customer's computer through Fleming-Mason's website.

Request 112. Refer to the Roush Testimony on behalf of Kentucky Power, DMR Exhibit 1. Provide a similar exhibit containing a list of time-differentiated rates available to your customers.

Response:

Residential and Small Power - Electric Thermal Storage Sch RSP-ETS

Request 113. Provide a description of the type of meters (mechanical, electro-mechanical, AMR [one-way communication], AMI [two-way communication]) currently used by the utility. Include in the description the reasons the current meters were chosen and any plans to move to a different type of metering configuration.

Response:

Mechanical	75%
Electromechanical	25%

AMI deployment scheduled for August, 2013. Please refer to PSC Case No. 2012-00361.

Request 114. If either AMR or AMI metering is in use, state whether the utility has received any customer complaints concerning those meters. If the response is yes, provide the following:

a. the number of complaints, separated by gas and electric if a combination utility, along with the total number of customers served.

b. how the complaints were addressed by the utility.

c. a detailed explanation as to whether customers should have the

ability to opt out of using either AMR or AMI metering.

d. If customers were to be given the opportunity to opt out of using either AMR or AMI metering, provide:

i. an explanation as to whether the utility should establish a monthly manual metering reading tariff or charge applied to the opt-out customers to recover the costs associated with manually reading the non-AMR or -AMI accounts.

ii. an explanation as to whether these opt-out customers could still receive benefit from the utility using either AMR or AMI metering.

iii. an explanation addressing the point at which opt-out customers, either in terms of number of customers or a percent of customers, affect the benefits of the utility using either the AMR or AMI metering.

Response:

Not Applicable

Request 115. In testimony, each utility cited cybersecurity as an area of concern related to the implementation of Smart Grid technologies. Provide and describe your company's policy regarding cybersecurity or the standard your company has adopted governing cybersecurity. If your company has not adopted any policy or standard, identify and describe any industry or nationally recognized standards or guidelines that you may be aware of that the Commission should consider relating to cybersecurity issues and concerns.

Response:

Fleming-Mason has not adopted a formal policy or standard but recognizes IEEE Standards.

Request 116. If not previously addressed, provide a detailed discussion of whether deployment of smart meters should allow for an opt-out provision.

Response:

Fleming-Mason would prefer that there be no opt-out provision. Smart meters are proven safe and the communication between the meter and the utility is invaluable in tracking usage, outages, voltage fluctuations, and anomalies that otherwise would not be detected. Smart meters allow for time-of-use rates, critical peak pricing, load control devices and other energy efficiency programs that benefit both the customer and the utility.

COMMONWEALTH OF KENTUCKY

BEFORE THE PUBLIC SERVICE COMMISSION

In re the Matter of:

CONSIDERATION OF THE IMPLEMENTATION	)	
OF SMART GRID AND SMART METER	)	CASE NO.
TECHNOLOGIES	)	2012-00428

FLEMING-MASON ENERGY COOPERATIVE, INC'S

RESPONSES TO ATTORNEY GENERAL'S
INTIAL DATA REQUESTS TO THE COMPANIES
DATED FEBRUARY 27, 2013

I, Christopher S. Perry, President & CEO, of Fleming-Mason Energy Cooperative, Inc., declare that the statements contained in this response are true to the best of my information and belief.

Christopher S. Perry, President & CEO
Fleming-Mason Energy Cooperative, Inc.

Subscribed and sworn to before me by Christopher S. Perry, this 18th day of March, 2013.

Notary Public, State-At-Large

My commission expires: June 20 2014.

Request 1. Since the Commission initiated Consideration of *the New Federal Standards of the Energy Independence and Security Act of 2007*, Administrative Case No. 2008-00408, has the company changed its position regarding Smart Grid? If so, how?

Response: Fleming-Mason references the response to AG Request 1 submitted by EKPC and adopts that response as its own.

Request 2. Are the technologies pertaining to the implementation of Smart Grid definitely known and proven?

a. If yes, explain in detail every aspect from the use of each technology from the company to the end-user.

b. If not, explain in detail what technologies are already advancing/improving as well as those that are envisioned on the immediate time horizon.

Response: Technology continues to evolve in the Smart Grid landscape. A prime example of that is AMI technology. A few years ago, power line carrier technology was the technology of choice for most Kentucky utilities but now there are sophisticated and robust RF systems available that may prove to be the way of the future.

Request 3. In light of resent catastrophic storms over the past ten years (for example, the various ice storms, tornadoes, and strong winds), which electric companies have experienced, and for which the company may ultimately have sought regulatory assets, can the company affirmatively state that its basic infrastructure, including all of its generation, transmission and distribution facilities, have proven to be reliable 24 hours a day, seven days a week, 365 days a week? If not, for each and every storm that it affected the utility in excess of two days, please provide the following:

Response: Fleming-Mason Energy has not requested a regulatory asset for recovery of costs for any major event or storms. The distribution system has proven to be reliable, but there are always events that may cause unexpected issues that may impact system reliability.

a. The number of days before the company's last ratepayer's electricity was restored for each storm.

Response:

Ice Storm May, 2009 7 days

b. The average number of days, or hours if applicable, that the average ratepayer's outage lasted for each storm.

Response: Not known.

c. The average financial loss for the average ratepayer for each storm, if known.

Response: Not known.

Request 4. Does the company agree with the Attorney General that electricity is not considered a luxury service but a necessary commodity of modern life? If not, why not?

Response: Fleming-Mason references the response to AG Request 4 submitted by EKPC and adopts that response as its own.

Request 5. Does the company agree that the fundamental reliability of its electric grid- i.e., the delivery of electricity to the end-user 24/7/365- is paramount to the end-user's ability to monitor and/or conserve his/her demand or electricity consumption? If not, why not?

Response: Fleming-Mason references the response to AG Request 5 submitted by EKPC and adopts that response as its own.

Request 6. Please state whether the company is aware of any cybersecurity breaches effecting the electric and gas industries that have either occurred in the United States or internationally. If the answer is in the affirmative, please explain the details of the breaches without exposing information that is not already in the public domain.

Response: No known.

Request 7. Please confirm that the company is aware that the prior United States Secretary of Defense Leon Panetta, in speaking on the vulnerability of the nation's electric grid with the consequential safety and security concerns that ensue, warned the Senate Appropriations Committee on Defense that the risk to the United States could even be considered the equivalent of a "digital Pearl Harbor".

a. Is this concern of the vulnerability of the nation's electric grid shared by the company? If not, why not?

Response: Fleming-Mason is aware that the nation's electric grid is of paramount importance for this country's ability to function. The vulnerability of the electric grid is of concern to Fleming-Mason.

Request 8. With regard to cybersecurity in general, can the company unequivocally confirm that its system reliability is not vulnerable to a cybersecurity attack? If not, what could be the consequences? Please explain in detail as much as possible for the following:

a. the company, and

b. the company's ratepayers.

Response: Fleming-Mason cannot unequivocally confirm that its system reliability is not vulnerable to cybersecurity attack. As a distribution cooperative, there are no generating assets therefore it could be assumed that Fleming-Mason would have minimal risk of a cybersecurity attack.

Request 9. Please provide the names of the standards, protocols or policies which the company observes and/or implements in its maintaining its system reliability from cybersecurity threats.

Response: Fleming-Mason observes IEEE cybersecurity standards when applicable.

Request 10. Please provide copies of the standards, protocols or policies which the company observes and/or implements in its maintaining its system reliability from cybersecurity threats.

Response: None available.

Request 11. With regard to cybersecurity in general, can the company unequivocally confirm that its ratepayers' privacy of data cannot be compromised or otherwise divulged to any individual or entity not associated with the company, or a qualified third-party which has issues a non-disclosure statement or the ratepayers? If not, what could be the consequences? Please explain in detail as much as possible for the following:

a. the company, and

b the company's ratepayers.

Response: Fleming-Mason follows The Red Flags Rule created by the Federal Trade Commission to confirm identity of its customers before connecting service. All data associated with customers is protected within the billing software under a robust firewall supported by our billing software vendor. To date, Fleming-Mason has not experienced any compromise of personal information of its customers

.

Request 12. If a qualified third-party that has agreed to a non-disclosure statement and obtains ratepayers' private information, what guarantees exist that the information will not be disclosed, whether intentionally or unintentionally?

Response: Fleming-Mason only deals with reputable vendors that meet the highest standards and feels confident that its customers' private information is well protected.

Request 13. Please provide the names of the standards, protocols or policies which the company observes and/or implements in its maintaining its ratepayers' privacy data from cybersecurity threats.

Response: Operating Policy No. 54: Identity Theft Prevention Program

Request 14. Please provide copies of the standards, protocols or policies which the company observes and/or implements in its maintaining its ratepayers' privacy data from cybersecurity threats.

Response: Attached – Exhibit 1

Request 15. Given the vulnerability of the electric grid to cyberattacks, describe what analog (non-digital) means the company will have in place to insure reliability, including but not limited to the maintenance of legacy systems.

Response: As an electric distribution system, the poles, wires, transformers, meters, etc. are all physical assets that are not vulnerable to cyberattacks. On the distribution system, most of the equipment can be bypassed at any time including system protection devices, metering, and regulation equipment to operate in a mode that would not be impacted. The billing software is duplicated daily at an off-site facility and could be recovered within hours of a catastrophic loss at Fleming-Mason's headquarters.

Request 16. What are the company's estimated costs to invest in order to fully implement Smart Grid?

a. Do any cost estimates include results of any modeling that may show the degree of exposure to the following risks: (a) hacking; (b) electronic magnetic pulses (EMPs, whether related to solar flares or otherwise); and/or (c) weather events? If so, provide a list of the modeling software used to produce any estimates, the scenarios and sensitivities examined, and any and all such results.

Response: Fleming-Mason references the response to AG Request 16 submitted by EKPC and adopts that response as its own.

Request 17. Please explain in detail what benefits, if any, the company expects its ratepayers to realize because of Smart Grid?

a. Does the company believe that societal benefits are to be considered in evaluating benefits? If so, detail those societal benefits and how they may be used in evaluations? If not, why not?

Response: Fleming-Mason references the response to AG Request 17 submitted by EKPC and adopts that response as its own.

Request 18 Would the company agree to strict limits and/or caps on ratepayer costs? If not, why not?

Response: Fleming-Mason references the response to AG Request 18 submitted by EKPC and adopts that response as its own.

Request 19. Would the company agree to allow ratepayers to opt-out of smart meter deployment? If not, why not?

Response: Fleming-Mason references the response to AG Request 19 submitted by EKPC and adopts that response as its own.

Request 20. Can the company quantify measureable and significant benefits that the ratepayers will realize, including a monetary quantification of net savings (if any) to ratepayers?

Response: Fleming-Mason references the response to AG Request 20 submitted by EKPC and adopts that response as its own.

Request 21. Please explain in detail what detriments, if any, the company expects its ratepayers to realize because of Smart Grid? Include in the explanation both new costs as well as stranded costs.

Response: Fleming-Mason references the response to AG Request 21 submitted by EKPC and adopts that response as its own.

Request 22. What are the company's estimated costs which the company expects the ratepayers to realize?

Response: Fleming-Mason references the response to AG Request 22 submitted by EKPC and adopts that response as its own.

Request 23. What are the company's estimated costs which the company expects its shareholders, if any, to realize? Include in the explanation both new costs as well as stranded costs.

Response: Fleming-Mason references the response to AG Request 23 submitted by EKPC and adopts that response as its own.

Request 24. Does the company agree that its costs to invest and implement Smart Grid will be different than other utility companies? If not, why not?

Response: Fleming-Mason references the response to AG Request 24 submitted by EKPC and adopts that response as its own.

Request 25. Does the company agree that its ratepayers' benefits, whether financial or otherwise, may differ from one utility to another upon implementation of any Smart Grid technology? If not, why not?

Response: Fleming-Mason references the response to AG Request 25 submitted by EKPC and adopts that response as its own.

Request 26. Can the company guarantee that the deployment of Smart Grid will not interfere with the regulatory compact whereby the ratepayers will receive safe, adequate and reliable service at fair, just and reasonable costs? If not, why not? Explain in detail.

Response: Fleming-Mason references the response to AG Request 26 submitted by EKPC and adopts that response as its own.

Request 27. Answer the above question with the definition of "fair, just and reasonable costs" as being economically feasible for the end-user.

a. Provide any cost-benefit analysis that the company has run or will run to make the determination of economically feasible to the end-user.

Response: Fleming-Mason references the response to AG Request 27 submitted by EKPC and adopts that response as its own.

Request 28. Regarding time of use (TOU) rates, can the company confirm that low-income ratepayers will not be disproportionately affected more than non-low-income customers? If not, why not? (Provide in the answers in any studies, reports, analyses and relevant data.)

Response: Fleming-Mason does not have any data to confirm either way.

Request 29. With regard to TOU rates, does the company have any history with any such programs? If so, explain in detail with particular facts as to:

a. the number of customers who participated;

b. whether they remained on the program;

c. whether they saved money on their bills; and

d. whether the customers ultimately reduced their usage.

Response: Fleming-Mason does not currently have any TOU Rates.

Request 30. What proposals will the company present to deal with technological impediments to the broad use of Smart Grid, including but not limited to the following:

a. low and fixed-income individuals who do not have Internet resources at their home;

Response: While internet in the home may offer more options for customers, it will not be a requirement to participate in Smart Grid programs. In-home displays could be offered as well as direct load control devices - neither of which require internet access.

b. multiple forms of telecommunications technology used to access information (i.e., analog, cellular, VOIP); and

Response: Phone Aps and text messaging are being integrated into current software applications when available.

c. multiple and proprietary technology and software options in the market that may lead to issues of compatibility?

Response: Fleming-Mason strives to maintain software that is compatible with the most prevalently used platforms.

Request 31. Assume: Full deployment of Smart Grid at the residential ratepayer level consisting of a household with only Energy Star appliances, an HVAC system with at least a 15 SEERS rating, etc. and any smart grid apparatuses/equipment for

interconnectivity with the electricity provider (including generation, transmission and distribution).

a. Does the company agree that if full deployment of the magnitude described in the above question occurs, the average residential ratepayer could experience a significant capital outlay?

b. If so, what are the projected costs?

c. If no costs are anticipated by the electric provider, why not?

Response: Fleming-Mason references the response to AG Request 31 submitted by EKPC and adopts that response as its own.

Request 32. In regard to appliances, such as refrigerators or lighting, does the company agree that in the long run, it is cheaper for the end-user himself/herself to make that capital outlay for the purchase of the appliance or lighting than have the company provide the appliance(s) and build the costs into the company's ratebase which would then include a profit component for the company on an on-going basis?

Response: Fleming-Mason references the response to AG Request 32 submitted by EKPC and adopts that response as its own.

Request 33. Confirm that the Smart Grid depends, at least in part, if not exclusively, on telephony (whether landline, fiber optic, wireless or VOIP) at the end-user level for the end-user to participate in his/her altering his/her electricity usage patterns or behavior.

Response: An in-home display is an option that would not require any type of telephony.

Request 34. If the answer to the above question is in the affirmative, confirm that limited access or even complete absence of access to telephony will interfere with, if not prevent, the deployment of the Smart Grid at the end-user level.

Response: Not necessarily.

Request 35. If the company intends to install infrastructure/software allowing for the transmission of Smart Grid/Smart Meter data over its distribution/transmission

conductors and networks, provide estimates, or actual numbers, for the costs of doing so.

Response: Not Applicable.

Request 36. Is there a standard communications' protocol that the company will deploy in its Smart Grid that will be interoperable regardless of the communications provider?

a. If not, explain how the company plans on addressing any problems that might arise.

Response: Yes.

Request 37. If improved reliability is the goal of Smart Grid/Smart Meter, would it not be more cost-effective to invest in infrastructure hardening (for example, utilizing protocols and standards developed and implemented by many utilities in hurricane-prone regions)?

Response: Fleming-Mason references the response to AG Request 37 submitted by EKPC and adopts that response as its own.

Request 38. Describe the company's plans to avoid obsolescence of Smart Grid/Smart Meter infrastructure (both hardware and software) and any resulting stranded costs. (This question and the subparts should be construed to relate to both the Smart Grid Investment Standard as well as the Smart Grid Information Standard.)

a. Describe who would pay for stranded costs resulting from obsolescence.

b. With regard to the recovery of any obsolete investment, explain the financial accounting that should be used (as in account entry, consideration of depreciation, time period involved, etc.).

Response: Fleming-Mason references the response to AG Request 38 submitted by EKPC and adopts that response as its own.

Request 39. With regard to interoperability standards, does the company agree that Smart Grid equipment and technologies as they currently exist, and are certain to evolve in the future, are not a one size fits all approach to the Commonwealth?

Response: Fleming-Mason references the response to AG Request 39 submitted by EKPC and adopts that response as its own.

Request 40. Is dynamic pricing strictly defined as TOU?

a. If not, explain why not.

b. Is the company requesting that dynamic pricing be voluntary or involuntary, if at all?

Response: Fleming-Mason references the response to AG Request 40 submitted by EKPC and adopts that response as its own.

Request 41. Please explain in detail whether the company has any dynamic programs in place in Kentucky.

a. For each program, provide the number of participants.

b. For each program, state whether those participants on aggregate have saved costs on their bills.

c. For each program, state whether those participants on aggregate have saved costs on their bills.

d. For each program, state whether each participant has saved costs on his/her/its bills. (The question is not intended to request any private identifier information.)

Response: Fleming-Mason does not currently have any dynamic pricing programs.

Request 42. Does the company recommend the Commission to formally adopt the EISA 2007 Smart Grid Investment Standard? If not, why not?

Response: Fleming-Mason references the response to AG Request 42 submitted by EKPC and adopts that response as its own.

Request 43. Does the company recommend the Commission to formally adopt the EISA 2007 Smart Grid Information Standard? If not, why not?

Response: Fleming-Mason references the response to AG Request 43 submitted by EKPC and adopts that response as its own.

Request 44. Does the company recommend issuing an IRP Standard?

a. If so, what concerns does the company have with a standard, including "priority resource," especially as it relates to cost-effectiveness?

b. What concerns would the company have with a standard as it affects CPCN and rate applications?

Response: Fleming-Mason references the response to AG Request 44 submitted by EKPC and adopts that response as its own.

Request 45. Does the company agree that any investment in grid modernization infrastructure should be done before deploying TOU rates or dynamic pricing? If not, why not?

Response: Fleming-Mason references the response to AG Request 45 submitted by EKPC and adopts that response as its own.

Request 46. Regarding the Kentucky Smart Grid Roadmap Initiative (KSGRI), does the company believe that it provides the fundamental basis for the Commonwealth as a whole to proceed with Smart Grid given its lack of incorporating all electric utilities such as municipalities and the TVA, along with its distribution companies? If yes, please explain why. If not, please explain why not.

Response: Fleming-Mason references the response to AG Request 46 submitted by EKPC and adopts that response as its own.

Request 47. Does the company believe that the Commonwealth's electric industry is, or will become, so interconnected that all electric entities in any way involved or associated with the generation, transmission and/or distribution of electricity should be

included and participate to some degree with Smart Grid if it is to come to fruition? If yes, please explain why. If not, please explain why not.

Response: Fleming-Mason references the response to AG Request 47 submitted by EKPC and adopts that response as its own.

Request 48. Does the company believe that any Smart Grid Investment will trigger a CPCN case? If not, why not?

Response: Fleming-Mason references the response to AG Request 48 submitted by EKPC and adopts that response as its own.

Request 49. Does the company believe that Dynamic Pricing should be economically feasible for the end-user and be supported by a cost- benefit analysis?

Response: Fleming-Mason references the response to AG Request 49 submitted by EKPC and adopts that response as its own.

Request 50. If additional education is contemplated with the deployment of the Smart Grid, please explain in detail if known or contemplated.

Response: Fleming-Mason references the response to AG Request 50 submitted by EKPC and adopts that response as its own.

Fleming-Mason Energy Cooperative, Inc.

Operating Policy No. 54

Subject: Identity Theft Prevention Program

Dated: November 1, 2008

Objective:

The goal of this policy is to prevent identity theft. Fleming-Mason Energy Cooperative, Inc. recognizes the responsibility to safeguard personal customer information within the workplace. The purpose of this policy is to create an Identity Theft Prevention Program utilizing guides set forth in the FACT Act (2003).

Scope:

This policy applies to management and all personnel of Fleming-Mason Energy Cooperative, Inc.

Responsibility:

Fleming-Mason Energy Cooperative, Inc. must protect customer data and implement policies and procedures that meet standards established by the Federal Trade Commission by November 1, 2008.

Definitions:

Identity Theft - Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, etc.) with the intent of conducting multiple transactions to commit fraud that results in substantial harm or inconvenience to the victim. This fraudulent activity may include opening deposit accounts with counterfeit checks, establishing credit card accounts, establishing line of credit, or gaining access to the victim's accounts with the intent of depleting the balances.

Company - For the purposes of this policy, Fleming-Mason Energy Cooperative, Inc. is referred to as Company.

Red Flag – A pattern, particular specific activity that indicates the possible risk of identity theft.

Procedure:

- Implementing the Program: Fleming-Mason Energy Cooperative, Inc. has developed an Identity Theft Program designed to detect, prevent and mitigate theft in connection with the opening or maintaining of any covered account. This program is consistent with the utility's mission to provide safe and reliable service at the lowest possible cost. *See Appendix I*
- Oversight of third party providers will assure that they also comply with the program.
- A privacy committee was formed with representation from key areas including: Management; Finance; Human Resources, Information Technology and Customer Service. It shall be the Privacy Officer's responsibility to maintain appropriate documentation of all meetings of the privacy committee. *See Appendix II.*
- Detailed documentation will be maintained by the Privacy Officer containing all pertinent information concerning the company's identity theft protection program, training, incident reports, etc.

Assessment of Company's Strength & Weaknesses:

The company has conducted a needs assessment of the flow of secured information during the processes of opening new accounts as well as monitoring transactions on existing accounts. The company also has evaluated internal and external identity theft risk in Information Technology security. A review of red flags in the industry and the examples outlined in the FACT Act legislation served as the basis for comparing present policies and procedures against those needed to detect, prevent and mitigate identity theft. *See Appendix I.* The company will continue to monitor strengths and weaknesses and will report to the Board of Directors on updates and/or changes in the assessment.

Handling Reports of Suspected Identity Theft:

When the Consumer suspects Identity Theft, he must notify the Company in writing, filling out the appropriate form *(See Appendix III).* Under the FACT Act, identity theft victims are entitled to a copy of the application or other business transaction records relating to their identity theft free of charge. Occasionally, a person or agency requests a consumer report on one of our customers. If this report includes an address that substantially differs from the addresses in the consumer's file, and a response to the request is issued, the Company should notify the person making the request of this discrepancy.

Identity Theft Training for Designated Employees

Designated employees will be trained on a "need to know" basis according to job responsibilities. The Cooperative will provide employees awareness training at least annually for employees with access to consumers' personal information, to ensure that employees are familiar with the provisions of this policy, including updates to the Program. Each employee will sign and date the attendance sign-in sheet. The Privacy Officer will preside in the training and verify attendance. New employees hired into positions handling secured information will receive initial training within thirty (30) days of employment date.

Reports, Reviews and Updates for Policy Enforcement

Periodically, internal staff and auditors who report to the board, external auditors and accountants, and government regulators will review practices to ensure compliance with corporate policy. The reports will be used to evaluate effectiveness of and amend the Identity Theft Prevention Program. An annual report reviewing all incidents, program revisions and goals will be submitted to the board of directors at the November Board meeting each year.

Board Approval

This policy is adopted by the Board of Directors as of November 6, 2008 and shall become effective on November 1, 2008.

Attested _____

Lonnie Vice, Secretary

APPENDIX I

Assess Company's Need for New/Updated Policies and Procedures

On October 6, 2008, Fleming-Mason Energy Cooperative, Inc. Identity Theft Prevention Program Committee conducted a needs assessment of the flow of secured information during the processes of opening new accounts and well as monitoring transactions on existing accounts. A review of red flags in the industry and the examples outlined in the FACT Act legislation served as the basis for comparing present policies and procedures against those needed to detect, prevent and mitigate identity theft. The following strengths and areas for improvement were identified:

Opening Accounts:

The assessed strengths for opening new accounts have been identified as the following:

- Semi-private areas are specifically designed to interview a new customer. This area is located several feet away from the lobby area decreasing the opportunity for others to overhear the confidential exchange of information. This also eliminates the possibility of someone looking over a shoulder to obtain personal information of a customer. Also, computer screens are not easily visible to those setting up a new service. Confidential information is not printed on service orders and written notes are shredded daily.

The assessed weaknesses for opening new accounts have been identified as the following:

- The Company not been verifying the identification of new customers. Effective November 1, 2008, the designated employees will have access to a 3rd party online verification service. This service will assist the designated employees with the proper tools to verify ID required.

Monitoring Transactions in Existing Accounts:

The assessed strengths for existing accounts have been identified as the following:

- Employees currently report suspicious activity on existing accounts to their supervisor. Before releasing information to a customer, the CSR will verify ID by asking for their social security number if the CSR has any doubt about the identity of the person they are speaking with.

The assessed weaknesses for existing accounts have been identified as the following

- Need to better utilize passwords and automatic screen savers; train employees to identity theft awareness; eliminate reports, passwords, paper/notes, etc. at each work station before leaving the premises; shredding all paper documents with customer information; securing the records retention area with key card access only (3rd parties NOT allowed).

Procedures:

Fleming-Mason Energy Cooperative, Inc. has developed the following procedures designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. All procedures represent a typical but not absolute response. Each situation can and will have circumstances, which will be affected by a number of variables.

The steps in establishing electrical service for a customer:

1. New service will be provided ONLY when identity of the member can be verified. New members must provide identification to the Company's designated employees which establish identity. The accepted documents have been defined by the FACT Act (2003) and acknowledged and accepted by the Identity Theft Prevention Program Committee of Fleming-Mason Energy Cooperative, Inc.

2. Effective, November 1, 2008 the Company will establish an online verification process which validates the social security number presented by the new consumer. The online verification process is provided by **Online Utility Exchange**. The designated employee will enter the prospective customer's social security number into the online verification system. In moments, the system will detect fraud, alerts, active duty alerts, and confirm credit for the new customer. The applicant may be required to also present a valid government issued photo identification as proof of identity.

3. In the event a new customer cannot come in to the office to apply for new service, the social security number must be provided to the designated employee. The designated employee will verify the social security number in the online verification system. The online verification system allows the designated employee to view previous address/addresses for the potential new customer.

4. In the event a new customer refuses to give the company his/her social security number, the customer must come to the office with only one document as listed below in Section 1. Otherwise, two forms of identity must be presented from the documents in Section 2:

SECTION 1:

a. U.S. Passport
b. Permanent Resident Card

SECTION 2:

a. Driver's license or ID card issued by a state provided it contains photo or info such as name, date of birth, gender, height, eye color and address.
b. Original or certified copy of birth certificate
c. U.S. social security card
d. U.S. Military card

The steps for sharing information for Existing Accounts:

Information will be shared with existing customers once identification has been verified by the designated employee. Verification can include the last 4 digits of the social security number, current address, current telephone number, account number or any combination thereof.

Training will be provided to supervisors and designated employees (customer service representatives and front line employees). This training will foster awareness of identity theft and prevention; outlines the basic difficulties affecting identity theft victims; and potential liabilities to the Company, Privacy Officer and designated employees.

Specific Identity Theft techniques will be shared by the Privacy Officer and local law enforcement officers on a need to know basis, required by the FACT Act (2003) and the policy.

Breech of Security

In the event of a breech of security, the following precautions will be taken to mitigate damage:

a. Notify supervisor
b. Secure the information
c. Define scope of the lost and/or stolen information (hard copy or information stored on computer.

Notification within the utility will be as follows:

a. The designated employee whom witnessed the alleged breech will report to Supervisor
b. The Supervisor will report to the Privacy Officer
c. The Privacy Officer will report the incident to the Chief Executive Officer.

At this time the Privacy Officer and the Chief Executive Officer will investigate the alleged breech of secure information. Reportable incidences will be reported to the appropriate law enforcement authorities and to the consumer/member. Customers affected by the breech will be contacted based on the scope and severity of the breech. If the breech of secure documents is severe, the Privacy Officer will contact the customer immediately by telephone. If the breech of secure documents is below severe to minimal (or null) the Company will notify the customer by certified mail outlining the specific details of the incident

APPENDIX II

Identity Theft Prevention Protection Committee:

On October 6, 2008, the Privacy Committee was formed under the leadership of Joni Hazelrigg, Chief Financial Officer.

Representation from key areas included:

Chris Perry – Chief Executive Officer
Joni Hazelrigg – Department of Finance
Natalie McKinney – Department of Human Resources
Pam Knipp – Department of Information Technology and Customer Service

The Committee members appointed Joni Hazelrigg as the Company's Privacy Officer on October 6, 2008.

Privacy Officer functions as the head of committee. He/she reports to the Chief Executive Officer regarding the outcomes and needs of the identity theft prevention program.

APPENDIX III

NOTICE OF IDENTITY THEFT - Fleming-Mason Energy

Consumer Submitting the Information:

Name: _____

Address: _____

_____

Date and Time of Receipt: _____

Verification of Consumer Identity: _____

Details of alleged ID theft: _____

_____

_____

Consumer Signature: _____

I acknowledge receipt of this notice.

Fleming-Mason Energy Employee: _____