SMUD™

LEG 2012-0426
June 27, 2012

Honorable Mary Nichols, Chair
California Air Resources Board
1001 I Street
Sacramento, CA 95814

Re: Sacramento Municipal Utility District's Comments on Proposed Modifications to California Cap on Greenhouse Gas Emissions and Market-Based Compliance Mechanisms Regulation

Dear Chair Nichols:

SMUD appreciates the opportunity to comment on the proposed amendments to the California Cap on Greenhouse Gas Emissions and Market-Based Compliance Mechanisms (Cap & Trade Program) rule. SMUD agrees with many of the proposed amendments. However, SMUD has a major concern with the proposed amendments related to the Know-Your-Customer (KYC) requirements in Sections 95830, 95834, 95912, and Appendix A.

SMUD understands that the main purpose for the proposed modifications is to prevent fraud by Authorized Account Representatives of Covered Entities registering for compliance accounts in the Cap & Trade Program. According to the Initial Statement of Reasons ("ISOR") published on May, 9, 2012, and discussions in the ARB Workshop of May 22, 2012, a key way to prevent fraud is to assure that the Authorized Account Representatives designated by Covered Entities are real people. And, in order to assure that account representatives are real people the ARB has proposed to adopt KYC practices from the banking industry. These requirements include, among other things, confidential information such as home addresses, phone numbers, social security numbers, and personal banking information. It is SMUD's understanding that, if adopted, this KYC information will be turned over to ARB's banker, Deutsche Bank. ARB staff has advised that the KYC checks are standard banking requirements, and for that reason should not be objectionable.

Although SMUD agrees with the goals of preventing fraud and securing market transactions, it must object to the means of using KYC requirements from the banking industry to protect individual customers to secure transactions by business-identified employees. SMUD believes that the ARB does not have the legal authority to justify disclosure of personal employee information either to itself or to its bankers, as a condition to participate in the Cap & Trade Program. SMUD also believes that the origin and common use of KYC information in the banking industry is inapposite to the need expressed in the regulations. Other commodity trading systems operate securely without requiring private information of the employees of regulated entities. As an

alternative, SMUD recommends using proven and less intrusive procedures from the energy markets or other regulatory programs.

I. The California Information Practices Act Precludes the ARB from Collecting and Maintaining the Personal Information Sought in Sections 95834 and 95912.

The proposed amendments to sections 95830(c)(2), 95834(b), and 95912(d)(5) (referencing Appendix A) violate the California Information Practices Act (the Act). The Act prohibits state agencies, such as ARB, from collecting personal information that is not relevant or not necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute.[1] The Act protects an individual's right to privacy from the indiscriminate collection, maintenance, and dissemination of personal information.[2] The Act implements strict limits regarding the collection and maintenance of personal information.[3]

Under the Act, the term "personal information" includes:

> any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.[4]

The "Know-Your-Customer" information listed in section 95834(b) and in Appendix A constitutes "personal information" under the Act because each request is for "information…that identifies or describes an individual." The data requested includes information expressly included in the Act's definition of "personal information" including: the individual's name, home address, social security number, employment history, driver's license number, and bank account information. Since ARB is a state "agency" under the Act, it is subject to the Act's "strict limits" regarding the maintenance and dissemination of personal information.[5] Consequently, ARB is prohibited from collecting the personal information sought in section 95834 and 95912 (referencing Appendix A), and sharing that information with Deutsche Bank, its banking contractor, if the

---

[1] Cal. Civ. Code § 1798.14 (Deering 2012).
[2] Cal. Civ. Code § 1798.1 (Deering 2012).
[3] *Id.*
[4] Cal. Civ. Code § 1798.3(a) (Deering 2012).
[5] The Act defines "agency" as every state office, officer, department, division, bureau, board, commission, or other state agency, except that the term agency shall not include: (1) The California Legislature. (2) Any agency established under Article VI of the California Constitution. (3) The State Compensation Insurance Fund, except as to any records which contain personal information about the employees of the State Compensation Insurance Fund. (4) A local agency, as defined in subdivision (a) of Section 6252 of the Government Code. Cal. Civ. Code § 1798.3(b) (Deering 2012).

information is not *necessary* for the Board to accomplish the Air Resources Board's statutory purpose.

According to the ISOR, the stated rationale of requiring the personal information is to identify the representatives of the covered entities who will participate in the cap and trade auctions.[6] The employee information sought by ARB to be delivered to Deutsche Bank is not *necessary* to identify the representatives of the registered entities because the registered entities themselves can confirm the identities of their employees, and because the ARB will approve the entities' registration and hold them financially accountable.[7] This is routinely done for traders in both the electric power and natural gas markets.

An alternative form of employee identification is a digital certificate. For its power market, the California ISO issues a digital certificate, which is installed on the trader's business computer. The digital certificate is unique to that trader and is necessary to make a trade and access other California ISO applications. The digital certificate, and unique password, can only be issued by a Certificate Authority, who is the California ISO for energy trades. For example, for SMUD to obtain a digital certificate, the point of contact in SMUD sends the ISO an application for access with the employee name and SMUD address, SMUD phone extension, and SMUD employee email address. No confidential, personal information is involved. Prior to renewal of the digital certificate, the ISO sends an expiration notice, which the SMUD point of contact either renews or cancels. The point of contact also cancels existing certificates when employees leave. The ISO sends the digital certificate directly to the individual via email, which checks the employee name against the SMUD global address list. The ISO copies the point of contact on this email, so if employee status were to change in the time from the request date, the point of contact can immediately cancel the certificate. The ISO will not issue a digital certificate unless the request comes from the authorized point of contact, who was delegated to that position by a SMUD manager.

Digital certificate identification assures counterparties, and the California ISO, that trades are only made by authorized representatives, without disclosing personal information of the trader to the ISO. A similar process could be used by the ARB with equal security, which would make disclosure of personal information unnecessary to confirm the identity of the Authorized Account Representative. The digital certificate also adds the level of security that would impede the possible hacking of the carbon market applications. Adoption of a digital certificate system would address security concerns underscored by the seven million Euro loss sustained in Europe in January of

---

[6] State of California Air Resources Board, *Staff Report: Initial Statement of Reasons, Proposed Amendments to the California Cap on Greenhouse Gas Emissions and Market-Based Compliance Mechanisms to Allow for the Use of Compliance Instruments Issued by Linked Jurisdictions* (May 9, 2012), available at http://www.arb.ca.gov/regact/2012/capandtrade12/isormainfinal.pdf.

[7] Cal. Code of Regs., tit. 17, §§ 95830, 05832 (2012).

2011.[8] Unidentified access to a user-name-and-password-only low level of security application is a high level concern but is not what's at issue here. Trading of GHG allowances and access to ARB Holding Accounts will be activities of business-identified employees.

Clearly, the Air Resources Board does not need the information sought under sections 95834 and 95912(d)(5) (referencing Appendix A) to confirm the identity of Account Representatives or their delegates. Specifically, the ARB does not need to obtain: (1) home address demonstrated by government-issued identity card, (2) date of birth, (3) passport, (4) driver's license, (5) criminal conviction record, (6) personal phone number, (7) email address, (8) social security number, (9) documentation of citizenship, and (10) documentation of an open bank account; all to simply identify an individual. Although this information makes identification more convenient for ARB staff, the information sought is not *necessary* for ARB to carry out the stated purpose of these regulations. The information requests listed in sections 95834 and 95912 represent the very type of indiscriminate collection and maintenance of personal information the Legislature sought to eliminate by enacting the Information Practices Act.

II. The Information Sought by the Air Resources Board in Sections 95834 and 95912 of the Proposed Amendments Subject Registering Entities to Liability for Invasion of Privacy Tort Actions.

The information requested by the ARB in sections 95834 and 95912(d)(5) opens up registering entities to potential liability from employee invasion of privacy tort actions. Specifically, the California Constitution explicitly guarantees an individual right of privacy. The California Constitution provides:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*. (Emphasis added).[9]

An individual's right to privacy is an inalienable right guaranteed explicitly by the California Constitution and such a right is legally enforceable.[10] The ARB's collection of the information sought in sections 95834 and 95912(d)(5) represents the kind of intrusion that the Legislature sought to protect with the Constitutional Amendment including: "(1) 'government snooping' and the secret gathering of personal information; (2) the overbroad collection and retention of unnecessary personal information by government and business interests; (3) the improper use of information properly

---

[8] *See* Nathanial Gronewold, *Europe's Carbon Emissions Trading – Growing Pains or Wholesale Theft?*, N.Y. Times, Jan. 31, 2011, available at http://www.nytimes.com/cwire/2011/01/31/31climatewire-europes-carbon-emissions-trading-growing-pai-74999.html?pagewanted=all.

[9] Cal. Const., art. I §1 (2012).

[10] *White v. Davis*, 13 Cal. 3d 757, 775 (1975).

obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party; and (4) the lack of a reasonable check on the accuracy of existing records."[11]

Because ARB provides no compelling interest necessary to warrant such an invasion of employee privacy, disclosure of this information by SMUD or other obligated entities risk civil actions by employees for violation of their constitutional right of privacy.[12] The California Court of Appeals for the First Appellate District has held that the "custodian of private information has the right, in fact the duty, to resist attempts at unauthorized disclosure and the person who is the subject of it is entitled to expect that his right will be thus asserted…[a]nd, of course, the custodian of such private information may not waive the privacy rights of persons who are constitutionally guaranteed their protection."[13] In sum, SMUD and other registering entities are not only concerned about wrongful disclosure and invasion of privacy, but are required to resist attempts at such unauthorized disclosures.

III. SMUD's Standard District Policies (SDPs) and District Administrative Procedures (DAPs) Preclude SMUD from Disclosing the Information Sought by the Air Resources Board in Sections 95834 and 95912(d)(5).

Pursuant to SMUD SDPs and DAPs, SMUD may not be able to disclose the information requested in sections 95834 and 95912 of the proposed amendments. Employee personnel information is defined by SMUD SDP 6.2.101 as "any information that personally identifies a SMUD employee including, home address, home phone number, cell phone numbers, birth date, health benefits, dependents, social security numbers, driver's license numbers, direct deposit banking information or financial accounts, personnel actions, background investigations, Department of Justice (DOJ) criminal history records checks, and personnel risk assessments."[14] SMUD classifies employee personnel information as sensitive and confidential information, and is therefore subject to SMUD information security policies.[15] SMUD employees must limit access to, and use of, sensitive and confidential information according to "need to know" and "minimum necessary" principles. SMUD will only disclose sensitive and confidential information if the use of the information is necessary to carry out official SMUD duties, and the disclosure is the minimum amount *necessary* to carry out official SMUD duties. SMUD's Board of Directors has adopted these policies in order to protect the legitimate privacy concerns of our employees.

---

[11] *Id.*
[12] The Court in *Board of Trustees, Stanford University v. Superior Court* held that the California Constitution protects employee personal information from improper disclosure to third parties. *Bd. of Trs., Stanford Univ. v. Superior Court of Santa Clara County*, 119 Cal. App. 3d 516 (1981).
[13] *Id.* at 526.
[14] SMUD SDP 6.2.101.
[15] *Id.*

The information sought by the ARB is neither necessary to carry out official ARB duties, nor would the disclosure be the minimum amount necessary to carry out official SMUD duties. Therefore, SMUD requests that these amendments be withdrawn to avoid a conflict with SMUD's information security policies.

IV. The Origin and Common use of KYC Information from the Banking Industry is Inapposite to the Need to Identify Authorized Account Representatives in the Cap & Trade Program.

Based on discussions from the ARB Workshop of May 22, 2012, it is SMUD's understanding that the "Know Your Customer" requirements were included in the proposed amendments at the request of Deutsche Bank. It is also SMUD's understanding that Deutsche Bank has required such information in its contract with ARB for financial services to support the allowance auction and various allowance holding accounts. While such protections may be required of institutions entrusted with financial securities, these protections are not required of commodities traders.

It appears to SMUD that Deutsche Bank may have incorporated requirements imposed upon it by the Securities and Exchange Commission ("SEC") into its dealings with the ARB. In early 2011, the SEC approved a proposal by FINRA, the Financial Industry Regulatory Authority, to adopt Know Your Customer rules. The new FINRA Rule 2090 was modeled after a former New York Stock Exchange rule, and requires securities firms doing business in the United States to use "reasonable diligence" in regard to opening and closing financial accounts, to know "the essential facts" concerning each customer and the authority of each person acting on behalf of such customers. The purpose of these rules is to ensure investor protection and to promote fair dealing and ethical sales practices.[16] Generally speaking, these rules apply to individuals and institutions who handle other people's money, such as "Introducing Brokers" and "Swap Dealers", in securities markets and banking. These rules were not written for commodity traders who trade for their own accounts, or those of their employers.

Another purpose of Know Your Customer policies is to prevent individuals from using financial institutions such as banks for illicit or illegal purposes. For example, in 1997 the Federal Reserve (the "Fed") republished its Bank Secrecy Manual, wherein it urged banks to adopt Know Your Customer policies to protect banks from criminal exposure. The Manual reads in pertinent part:

[16] Financial Industry Regulatory Authority, Regulatory Notice 11-02: Know Your Customer and Suitability, FINRA (Jan. 2011), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p122778.pdf.

> Even though not presently required by statute, it is imperative that financial institutions adopt "know your customer" guidelines or procedures to ensure the immediate detection and identification of suspicious activity at the institution."[17]

While the Fed finds it appropriate for banks to adopt KYC policies for opening and closing bank accounts, the Cap & Trade Program is a closed system, unlike the currency system in the banking industry. Registering entities cannot, for example, move allowances from the illegal drug trade through an ARB allowance Holding Account, to be sold at a later time to a gun running operation overseas. Allowances are simply not that fungible. The need of banks to know their customers flows from the fact that currency is legal tender and can be used for a myriad of purposes and goods. Emission allowances are created by ARB, tracked in accounts that will be monitored by ARB, and for the very limited use of paying ARB for the right to emit GHG emissions. There is simply no parallel security risk by Covered Entities, or other registered entities, on whose behalf Authorized Account Representatives trade.

There are numerous examples in commodity markets of trading platforms that can be used to assure ARB that employees or agents of registered entities are authorized to trade on behalf of their organizations. SMUD mentioned above the digital certificate system used by the California ISO. Another model is the internet-based market used to trade energy contracts, known as ICE.[18] SMUD uses ICE to trade hundreds of millions of dollars in power and gas contracts every year. ICE requires that SMUD approve a list of traders, then issue a user name and password for each authorized trader. Those users individually have credit limits and the organization has credit limits as a whole. Positions cannot be put on in excess of those limits, nor can individuals trade on behalf of the organization without permission. The organization has the responsibility for trader activity, not the trader. The organization provides the information necessary to satisfy ICE, and other market participants, that it can trade. ICE has operated successfully for years without requiring confidential, personal information from traders.

In summary, the KYC requirements proposed to sections 95830(c)(2), 95834(b), and 95912(d)(5) (referencing Appendix A) are unnecessary and inappropriate to fulfill

---

[17] Federal Financial Institutions Examination Council, Bank Secrecy Act Manual § 601.0, FFIEC (1997), *available at* http://www.federalreserve.gov/boarddocs/SupManual/bsa/bsa_p5.pdf. The most recent (2010) Bank Secrecy Act Manual continues to reference to "Know Your Customer" practices, now termed "Customer Identification Program", which is implemented by the Patriot Act. ARB has never suggested that its Know Your Customer requirements are being required as a matter of national security under the Patriot Act. As stated in the manual, although banks are required to have a customer identification program, the program is focused at customers opening bank accounts. Specifically, the CFR and Manual provide that at a minimum, the bank must obtain the following identifying information from each customer before opening the account: Name, Date of Birth, Address, Identification number. *See* Federal Financial Institutions Examination Council, Bank Secrecy Act Manual 54, FFIEC (2010), *available at* http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf.

[18] ICE is actually an American financial company called International Exchange, Inc. Natural gas, power and even carbon emissions (EU allowances) are traded on ICE's web-based exchanges.

the need for ARB to ensure the identity of authorized account representatives with access to allowance auctions and allowance holding accounts. Requesting this information as a condition for participation in the Cap & Trade Program is not authorized by law, and potentially subjects registered entities such as SMUD to employee lawsuits for violations of state privacy protections. It also violates the values and policies of SMUD. Therefore, SMUD urges the ARB to reconsider these regulations and adopt more customary practices for secure commodity trading in the energy industry.

SMUD again appreciates the opportunity to comment on the May 9, 2012 modifications to the California Cap on Greenhouse Gas Emissions and Market-Based Compliance Mechanisms Regulation, and urges consideration of the comments described above.

/s/

_____

WILLIAM W. WESTERFIELD, III
Senior Attorney
Sacramento Municipal Utility District
P.O. Box 15830, M.S., B406, Sacramento, CA 95852-1830

/s/

_____

TIMOTHY TUTT
Government Affairs Representative
Sacramento Municipal Utility District
P.O. Box 15830, M.S. B404, Sacramento, CA 95852-1830

/aa
cc: Corporate Files