

Important- Cap-and-Trade Information Security Email

December 27, 2012

Dear Primary Account Representative:

You are receiving this email because you are designated as a Primary Account Representative in the Compliance Instrument Tracking System Service (CITSS) for an entity registered under the California cap-and-trade program (Sections 95800 to 96023, Title 17, California Code of Regulations).

The purpose of this email is to remind you and your organization of prohibitions on the release of certain information, and to strongly advise you to maintain effective control of your program data and credentials. Please read this email carefully and in its entirety. If you have any questions about the information in this email or regulatory requirements, please contact Ms. Rajinder Sahota, Manager, Program Monitoring Section, at (916) 323-8503 or rsahota@arb.ca.gov.

Prohibitions on the Release of Certain Information

The California cap-and-trade program includes periodic auctions of emission allowances. How an entity may purchase allowances at auction is described in program guidance available at: <http://www.arb.ca.gov/cc/capandtrade/guidance/guidance.htm>.

The auction design and the rules for participation were established to ensure the integrity of the auction, including fair and equitable access for all qualified auction participants. *Among the requirements for auction participants is the prohibition on the release of an individual entity's auction information, including information on auction participation (section 95912 (f)) and information on bid qualification status, bid price or bid quantity, the bid guarantee provided to the financial services administrator, and other information identified as confidential information in the auction application by the auction administrator (section 95914 (c)(1)).*

These prohibitions on the disclosure of this auction information are explained in the program guidance referenced above. It is important that you as the Primary Account Representative be familiar with these prohibitions, and that you ensure your organization is familiar with them as well.

Maintain Effective Control Of Your Program Data

ARB strongly encourages you to ensure that your organization maintains and follows written procedures and policies that provide effective control of your program information. Controlling access to all of your program data protects your organization as well as all program participants. Also, the information listed in section 95912 (f) and section 95914 (c)(1) must be controlled to avoid being in violation with the program requirements. ARB will evaluate any release of such information for possible enforcement action.

If you suspect that your program information has been accessed by unauthorized individuals, ARB strongly encourages you to investigate how the unauthorized access occurred and to improve your procedures and policies to prevent future unauthorized access. ARB also strongly encourages you to notify ARB of the unauthorized access immediately. If any information listed in section 95912 (f) and section 95914 (c)(1) is released for any reason, we request that you immediately notify ARB of the situation at the contact information provided above.

Maintain Effective Control Of Your Program Credentials

ARB strongly encourages you to ensure that your organization maintains and follows written procedures and policies that provide effective control of your program credentials that provide your organization access to CITSS and the Auction Platform. As you know, unauthorized access to your organization's accounts in these systems could harm you and possibly other program participants.

- Please be aware that account credentials are tied to a unique individual, at no point should they be shared with another person (section 95834).
- Under California's regulation, account representatives are responsible for any action undertaken with their account credentials. (section 95832 (a)(4) and section 95832 (c)(2))
- Violation of these provisions or the CITSS Terms of Use may result in removal of a user's access to CITSS or other enforcement measures. (CITSS Terms of Use:

http://www.arb.ca.gov/cc/capandtrade/markettrackingsystem/forms/2_user_registration_form.pdf)

ARB also recommends that your organization's staff is properly trained to recognize potential threats from cybercriminals. Information is available from the Federal Bureau of Investigation (<http://www.fbi.gov/about-us/investigate/cyber/cyber>) to help you understand cybercrime risks and how to prepare.

If You Suspect That Your Credentials Have Been Compromised

ARB has received no reports of credentials being compromised for CITSS or the Auction Platform. If each participating organization maintains effective control of their credentials, no such events will occur.

If at any time you suspect that the credentials that provide you and your organization access to CITSS or the Auction Platform have been compromised, take steps immediately to prevent unauthorized access to these systems.

- Contact your IT support group and follow your organization's procedures for reporting and resolving the situation.
- Contact CITSS Help Desk to report the situation at 1-866-682-7561 or help@wci-citss.org and immediately reset the passwords for all your organization's account representatives and viewing agents for CITSS and the Auction Platform.

- File a complaint with appropriate law enforcement officials in your area. You may also want to file a complaint with The Internet Crime Complaint Center (IC3) (<http://www.ic3.gov/default.aspx>).

Confirmation of Receipt of Email (Action Required)

ARB is requesting all Primary Account Representatives to acknowledge receipt and reading of this email by responding via email to Mr. David Kennedy at dkennedy@arb.ca.gov by January 11, 2013; 5 PM PT.

Thank you for your attention to the matters in this email. If you have any questions about the information in this email, please contact Ms. Rajinder Sahota using the information provided above.