



governmentattic.org

"Rummaging in the government's attic"

Description of document: Commodity Futures Trading Commission (CFTC)
document POL-OED-ESB-2: CFTC Policy: Responding to
Incidents Involving CFTC Confidential Information, 2015

Requested date: 24-February-2017

Released date: 27-February-2017

Posted date: 10-July-2017

Source of document: FOIA Compliance Office
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581
[Online FOIA Request Form](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



FOIA Office

U.S. COMMODITY FUTURES TRADING COMMISSION

Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
www.cftc.gov

February 27, 2017

RE: 17-00061-FOIA
A copy of the document: CFTC
Policy: Responding to Incidents
Involving CFTC Confidential
Information

This is in response to your request dated February 24, 2017, under the Freedom of Information Act seeking access to a copy of the document: CFTC Policy: Responding to Incidents Involving CFTC Confidential Information. In accordance with the FOIA and agency policy, we have searched our records, as of February 24, 2017, the date we received your request in our FOIA office.

We have located 6 pages of responsive records. I am granting partial access to, and am enclosing copies of, the accessible records. Portions of some pages fall within the exemptions to the FOIA's disclosure requirements, as explained below.

Some records contain information the disclosure of which could reasonably risk circumvention of the law. This information is exempt from disclosure by FOIA Exemption 7(E). 5 U.S.C. § 552(b)(7)(E).

You may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001, email at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.


If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 8th Floor, 1155 21st Street, N.W., Washington, D.C. 20581, within 90 days of the date of this letter. Please enclose a copy of your original request and a copy of this response.

If you have any questions about the way we handled your request, or about our FOIA regulations or procedures, please contact Tameka Tilliman at 202-418-5091.

Sincerely,

A handwritten signature in cursive script, appearing to read "Candace Ambrose".

Candace Ambrose
Counsel

	CFTC Policy: Responding to Incidents Involving CFTC Confidential Information
Division/Branch:	OED/Executive Secretariat Branch/Privacy Office ODT/Policy and Planning Branch OGC/General Law
Description:	Policy for reporting and responding to incidents that may involve CFTC confidential information, including personally identifiable information
Policy Number:	POL-OED-ESB-2
Date Approved:	September 25, 2015
Approved By:	Chairman Timothy Massad
Certified By:	Anthony C. Thompson, Executive Director John Rogers, Chief Information Officer Jonathan Marcus, General Counsel
Supersedes:	CFTC Policy: Personally Identifiable Information Breach Notification CFTC Policy: Reporting Incidents Involving Personally Identifiable Information
Contact:	Kathy Harman-Stokes, Chief Privacy Officer (CPO), x6629 Naeem Musa, Chief Information Security Officer (CISO), x5485 Joan Fina, Assistant General Counsel for General Law, x7621

I. Purpose

To accomplish its mission, the CFTC collects, maintains, uses, and shares confidential information¹ including but not limited to confidential business information, internal non-public deliberations, and personally identifiable information (PII), and must handle this information in accordance with legal requirements.² However, agencies also must plan for a potential loss of control and respond accordingly to protect the agencies and individuals who may be affected.

The purpose of this policy and related guidelines and attachments (collectively "Confidential Information Incident Response Plan" or "IRP") is to set forth the CFTC's obligations for containing, investigating, reporting and responding to confidential information incidents. The IRP addresses the reporting of potential incidents and incidents by staff to an internal CFTC Incident Response Team (IRT), the IRT's reporting to the General Counsel, Senior Agency Official for Privacy (SAOP), and Chief Information Officer (CIO). The IRP also

¹As explained in OGC Memoranda: [Handling and Disclosure of Confidential Information](#), see Definitions Section III, information is considered confidential when its unauthorized disclosure would adversely impact:

- a person's privacy or welfare,
- the CFTC's mission, business or operations, or
- another government agency or private entity's mission, business, or operations.

² Confidential information must be protected pursuant to the Commodity Exchange Act, Privacy Act of 1974 and other applicable laws, and pursuant to CFTC obligations to third parties through agreements, memoranda of understanding and international arrangements with foreign regulators.

addresses additional reporting as appropriate to internal stakeholders, such as the Chief of Staff, Office of Legislative Affairs, Office of Public Affairs, and Office of Inspector General, and external stakeholders, including to US-CERT, banks that may hold credit cards that have been compromised, law enforcement, Congress, and the public.

The IRP further addresses the assessment of risk and considerations for possible notification to firms or individuals whose information may have been compromised. This policy is designed to minimize the risks to CFTC, its registrants and the financial markets the CFTC oversees, and risks to individuals whose information the CFTC holds from the impacts of a potential loss of control of or unauthorized access to confidential information, and when an incident occurs, to efficiently and effectively contain the incident, investigate it, engage stakeholders and minimize risks.

This document applies to all confidential information under the purview of CFTC, whether in paper or electronic form, and whether held by any CFTC employee, contractor, consultant, volunteer, or intern (unless the context shows otherwise, collectively “staff”).

II. Application

COMPLIANCE WITH THIS POLICY IS MANDATORY FOR ALL CFTC STAFF

III. Policy

A. Definitions

Please review the following definitions to understand the method for reporting incidents and the roles and responsibilities:

1. **Confidential information (CI)** is information that, if disclosed without authorization, would adversely impact: a person’s privacy or welfare; the CFTC’s mission, business or operations; or another government agency or private entity’s mission, business, or operations.
2. **Personally Identifiable Information (PII)** is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. This definition does not distinguish levels of sensitivity of the PII and is intended to be broad and all-encompassing.
3. **Sensitive personally identifiable information (Sensitive PII or SPII)** is a subset of PII, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, including possibly identity theft. Sensitive PII is considered CFTC confidential information.
4. **An Event or potential incident** is an observable change to the normal behavior of, or deviation from applicable law or regulations related to, a system, environment, process, workflow or person that is deemed to be suspicious. An event may suggest that an incident has taken place. Staff must report all events to the IRT as stated herein.
5. **An Incident** is the **actual or suspected** loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to confidential information, whether physical or electronic. [\[OMB M-07-16.\]](#)

6. **Incident Response Team (IRT)** includes those individuals identified in the [Incident Response Team Guidelines](#), at a minimum the Chief Privacy Officer, Chief Information Security Officer (CISO), Chief of Workforce Relations, designated Assistant General Counsel for General Law, and ODT Security Operations Manager. Other individuals may participate with the team on an ad hoc basis, as needed, e.g., the CFTC Chief Security Officer will participate whenever an incident involves physical security of facilities or personnel.
7. **Senior Leadership Response Team (SLRT)** includes those individuals identified in the [Senior Leadership Response Team Guidelines](#), at a minimum, the General Counsel, Chief Information Officer (CIO), and Senior Agency Official for Privacy (SAOP). The SLRT may add other staff as appropriate.

B. Reporting Incidents

CFTC staff shall:

1. Report any potential incident or incident to the CFTC IRT by contacting (b)(7)(E) or through other means as stated on the CFTCnet "Privacy Program" page, as soon as possible after the potential incident is observed.
2. If a contractor, also report the potential incident or incident to the Contracting Officer (CO) and Contracting Officer's Representative (COR).
3. If a staff member would like to report a potential incident or incident anonymously, the staff member may provide information about the potential incident or incident on paper via interoffice mail addressed to "CFTC Potential Incident," or hand delivery to any member of the IRT or the "CFTC Potential Incident" mailbox in the DC HQ library. Please note that reporting a potential incident or incident through this method may hinder the IRT's ability to quickly and fully respond to the potential incident or incident.
4. Include in the report the information stated in CFTC Form: Report of a Potential Incident or Incident that May Involve Confidential Information, attached to this policy.

C. Roles and Responsibilities

1. The CFTC IRT shall follow the IRT Guidelines, including determining whether a potential incident constitutes an incident under CFTC policies, containing incidents, deploying damage control procedures, investigating, and ensuring appropriate forensic analysis and reporting.
2. The CIO's designee shall report incidents to the [DHS Computer Emergency Readiness Team \(CERT\)](#) as needed under applicable information technology rules or guidelines.
3. The Chief of Workforce Relations is responsible for coordinating labor and employee relations activities relating to an incident.
4. The SAOP, CIO, and General Counsel shall follow the Senior Leadership Response Team Guidelines (SLRT Guidelines), including ensuring that the IRT properly responds to the incident, reviewing reports from the IRT, adding other subject matter experts to the SLRT to assist in handling particular incidents, notifying appropriate stakeholders of an incident, taking action to minimize harm to any affected individuals or firms, and supporting efforts to prevent similar incidents in the future.
5. The SAOP is responsible for deciding whether the agency will notify and, if appropriate, provide other assistance such as credit monitoring to individuals who could be impacted by an incident that may involve PII, in consultation with the CIO and General Counsel, and based on recommendations from the Chief Privacy Officer and applicable law, guidelines and best practices.

6. The General Counsel is responsible for deciding whether the agency will notify firms or other third parties which could be impacted by an incident that may involve that party's information, in consultation with the CIO and SAOP, and based on recommendations from the designated Assistant General Counsel for General Law on the IRT.
7. CFTC supervisors are responsible for ensuring that their staff are aware of the procedures for responding to potential incidents and the content of other CFTC security and privacy policies that help to prevent the occurrence of incidents (e.g., limited personal use policy, Safeguarding PII policy, and OGC Memorandum on Handling and Disclosure of Confidential Information).
8. Contracting Officers and the Chief of the Financial Management Branch procurement team are responsible for ensuring that contracts under their authority contain appropriate incident response guidelines, and for verifying that contractors are aware of the procedures for responding to potential incidents and the content of other CFTC security and privacy policies that help to prevent the occurrence of incidents (e.g., limited personal use policy, Safeguarding PII policy, and OGC Memorandum on Handling and Disclosure of Confidential Information). They also are responsible for ensuring that contractor staff participate in regular privacy and security training.
9. The Director, Logistics and Operations Section is responsible for assisting in incident response activities involving building or other physical security and contacting law enforcement when appropriate.
10. The Office of the Inspector General (IG) may receive reports of incidents from the IRT and/or the SLRT, typically at the conclusion of an investigation, at the discretion of the IRT and the SLRT.
11. The IRT shall ensure that CFTC staff, including members of the SLRT, are annually trained in this policy and their specific responsibilities.

IV. Confidentiality of Information Related to a Potential Incident or Incident

Any information related to a potential incident or incident could include sensitive PII or other CFTC confidential information; therefore, the potential incident or incident itself shall be treated as confidential and communications should be limited to staff who need to know about an incident to perform their job duties unless the IRT or SLRT members instruct otherwise. Any CFTC staff who become aware of a potential incident or incident and have reported the situation to the IRT, whether or not he or she is involved in the CFTC response to such potential incident or incident, may not disclose any information concerning the potential incident or incident to any other CFTC staff or to any third parties, unless specifically authorized by members of the IRT or SLRT. Only the CFTC Office of Public Affairs, the Chairman or Commissioners may discuss any potential incident or incident with media. Notwithstanding the foregoing, a member of a bargaining unit may consult with or be represented by a union representative in accordance with federal law or any applicable bargaining agreement. The union representative would be subject to CFTC and Federal ethical confidentiality requirements, as well as privacy requirements under the Privacy Act of 1974.

In accordance with the Privacy Act and the Federal Records Act, all records related to a potential incident or incident that may involve PII shall be generated, compiled and maintained in a manner sufficient to safeguard the financial, legal or other rights of individuals, if any, affected by the incident, including any parallel law enforcement investigations, litigation, or other pending action. Such records will be destroyed in accordance with approved and secure methods designed to ensure against inadvertent disclosure, theft, or other compromise of personal or other nonpublic information.

V. Regular Reviews of this Policy

The IRT shall ensure that this policy, related guidelines and documents are reviewed at least every other year and updated as needed. The IRT also shall ensure that, at least once every two (2) years, the IRT and SLRT engage in incident response training and practice of this policy and its guidelines in an effort to improve their effectiveness.

VI. Consequences of Failure to Comply

Employees: Failure to comply with this policy could result in the loss of use or limitations on use of information technology resources; remedial action in the form of a reprimand, suspension, removal from federal service; and/or criminal penalties in accordance with federal law and regulations.

Contractors, consultants, interns and volunteers: Failure to comply with this policy could result in the loss of use or limitations on use of information technology resources; withholding of payment for services (if applicable); replacement of personnel under a contract; termination of the contract or services; and/or other remedies that may be available under law.

VII. Other Authorities

- [The Privacy Act of 1974](#)
- [Federal Information Security Management Act of 2002](#)
- [Commodity Exchange Act, 7 U.S.C. §§ 1 et seq.](#)
- [Privacy Act of 1974, 5 U.S.C. § 552a](#)
- [OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Budgets](#), July 12, 2006.
- [OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information](#), May 22, 2007

VIII. Related policies, procedures and forms:

- CFTC Form: Report of a Potential Incident that May Involve Confidential Information
- CFTC Incident Response Plan, including:
 - CFTC Guidelines: Incident Response Team
 - CFTC Guidelines: Senior Leadership Response Team
 - Supplemental Documents (contact information for IRT and SLRT, sample notices, etc.)

CFTC Form: Report of a Potential Incident or Incident that May Involve Confidential Information

INSTRUCTIONS: CFTC staff shall report any potential incident or incidents to the CFTC Incident Response Team (IRT) by contacting (b)(7)(E) or through other means as stated on the CFTCnet "Privacy Program" page, as soon as possible after the potential incident is observed. Staff may use this form, may copy the below table into an email, or may report the same information in a different form.

If a staff member would like to report a potential incident anonymously, the staff member may provide information about the potential incident on paper via interoffice mail addressed to "CFTC Potential Incident," or hand delivery to any member of the IRT or the "CFTC Potential Incident" mailbox in the DC HQ library. Please note that reporting a potential incident through this method may hinder the IRT's ability to quickly and fully respond to the potential incident.

When filled out, the information contained on this form should be kept confidential under CFTC policy, and only disclosed as authorized under CFTC policy.

* * * * *

REPORT OF A POTENTIAL INCIDENT OR INCIDENT THAT MAY INVOLVE CONFIDENTIAL INFORMATION

**CONFIDENTIAL – DO NOT DISCLOSE WITHOUT SPECIFIC AUTHORIZATION
MAY CONTAIN CONFIDENTIAL INFORMATION, INCLUDING PII**

*First and last name of reporting staff: _____	*Division/Office of reporting staff: _____	*[] Employee (includes interns, volunteers, etc.) [] Contractor (includes consultants)
Date of report: _____	[] WDC [] NYC [] CH [] KC	
*Contact email address: _____	*Contact phone number: _____	*Alternate phone number: _____
Date of potential incident: _____	Time of potential incident: _____	Location of potential incident: _____
If the information may have been stolen, have you contacted law enforcement? [] Yes [] No	If you contacted law enforcement, please provide contact info of law enforcement: _____	
Form of information that could be at risk: [] Physical [] Electronic [] Other (e.g., flash drive) _____		
Describe the potential incident in detail. Provide additional pages if necessary. Example, "I arrived at home and realized that I had left my briefcase on the Metro; the briefcase contained a CFTC iPad and paper files with trade position data."		
Describe the types of CFTC confidential information, including but not limited to personally identifiable information, that could be at risk and number of firms or individuals who could be affected. Example, "The paper files included trade positions, and info on the individual owners of those positions, in a specific market. There are 7 firms operating in that market. The iPad contains . . ."		
Add any other information you feel may be useful to the Incident Response Team:		

**You may omit this information and report a potential incident anonymously, but please note that reporting anonymously may hinder the IRT's ability to quickly and fully respond to the potential incident.*