



Privacy Impact Assessment for LabCFTC

6/11/2020

System/Business Owner

Bianca M. Gomez

Reviewing Official

Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

I. SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

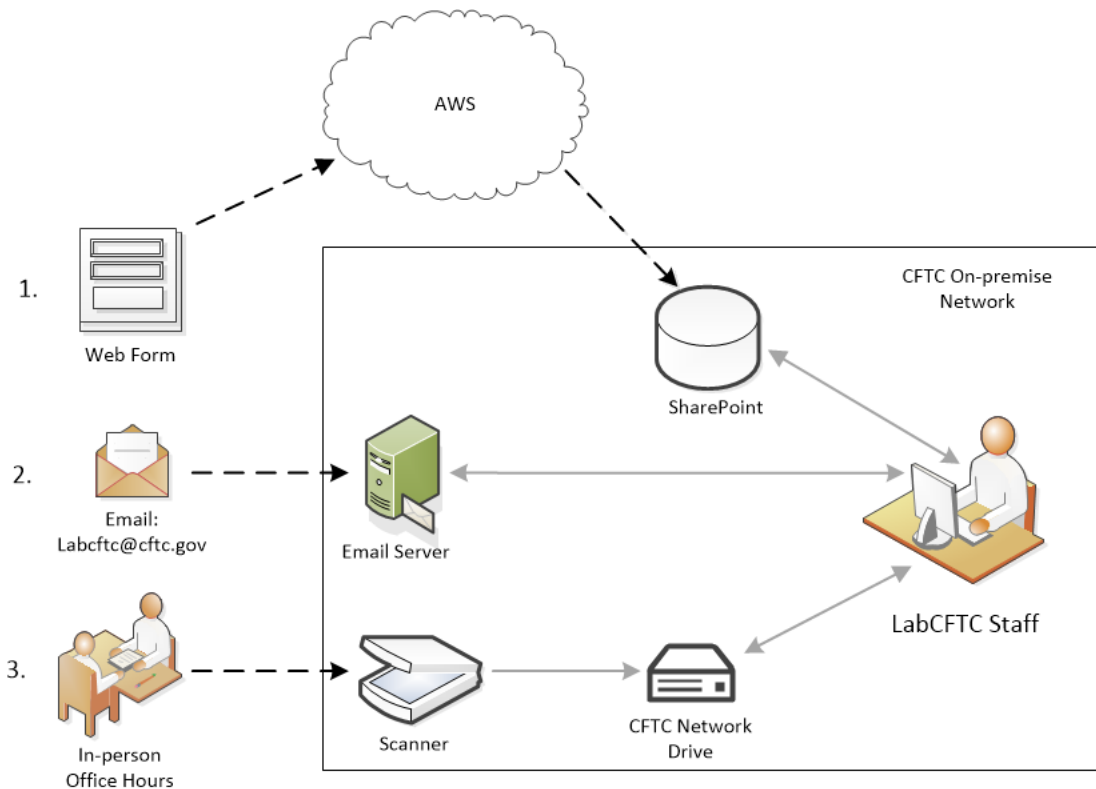
In service to the CFTC's goal of encouraging innovation and enhancing the regulatory experience for market participants at home and abroad, the CFTC established LabCFTC, an official operating office that reports directly to the Chairman of the Commission. LabCFTC's mission is to promote responsible innovation among the financial industry, stakeholders, and policymakers by:

- Advancing policy and regulation in financial innovation;
- Facilitating dialogue between innovators and those within the CFTC on financial and technological innovations;
- Educating internal and external stakeholders on financial technology and innovation in the financial markets to identify how innovations are being used; and
- Coordinating internally and externally with international, federal, and state regulators, organizations, and associations.

LabCFTC is designed to make the CFTC more accessible to FinTech innovators and serves as a platform to inform the Commission's understanding of new technologies. LabCFTC allows FinTech innovators to engage with the CFTC, learn about the CFTC's regulatory framework, and obtain feedback and information on the implementation of innovative technology ideas for the market. Further, LabCFTC functions as an information source for the Commission and CFTC staff on responsible FinTech innovation that may influence policy development. LabCFTC facilitates FinTech innovators engaging with the CFTC, learning about the CFTC's regulatory framework, and obtaining feedback and information on the implementation of innovative technology ideas for the market.

LabCFTC collects personal information through in-person office visits (LabCFTC office hours), through the Labcftc.gov email address, through the secure online office visit scheduling form located on the Labcftc.gov web site, and through prize competitions authorized under the American Innovation and Competitiveness Act.

2) Provide a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Include a brief description of the data flows.



FinTech industry participants contact and submit personal information to LabCFTC through the following three mechanisms. While personal information may be collected through each of these mechanisms, the information is ultimately stored on an access controlled LabCFTC network drive accessible by LabCFTC staff.

1. **Web Form:** The web form collects contact information that is necessary to correspond with the submitter. Through the web form, submitters may also upload additional files to supplement their inquiry or request. Submitter information is temporarily stored on the secure webserver, hosted by Amazon Web Services (AWS), until its receipt and validation can be confirmed by CFTC’s backend systems. Once the data has been validated and transferred to the LabCFTC SharePoint site, the data on AWS is securely deleted. Certain non-personal information is retained on the web server, including a log of dates of submissions, submission types and subtypes. This information is necessary for verification and system operation purposes.
2. **Labcftc@cftc.gov:** Individuals who contact LabCFTC through the program’s dedicated e-mail address typically include their business contact information in the communication. Individuals choosing to schedule In-person Office Hour visits by e-mail instead of using the web form provide the same personal information that would be collected had they opted to use the web form. Only LabCFTC staff have access to the program’s dedicated mailbox.

3. In-person Office Hours: Individuals who make an appointment to visit LabCFTC staff in person during LabCFTC office hours often bring printed materials with them that include business contact information. Printed materials that are provided during the office visit are scanned into digital format and saved on the LabCFTC SharePoint site or network drive.

II. AUTHORITY AND PURPOSE

- 1) What is the legal authority to collect, use, maintain, and share information in the system?

The collection of this information is authorized under 7 U.S.C. 5(b). Information collected to facilitate competitions is authorized under the American Innovation and Competitiveness Act (AICA) P.L. 114-329.

III. INFORMATION TYPES

- 1) What information will be collected, maintained, used, and/or disseminated?

Identifying Numbers	
<input type="checkbox"/> Social Security Number	<input type="checkbox"/> Truncated or Partial Social Security Number
<input type="checkbox"/> Driver’s License Number	<input type="checkbox"/> License Plate Number
<input type="checkbox"/> Patient ID Number	<input type="checkbox"/> File/Case ID Number
<input type="checkbox"/> Student ID Number	<input type="checkbox"/> Health Plan Beneficiary Number
<input type="checkbox"/> Passport Number	<input type="checkbox"/> Federal Student Aid Number
<input type="checkbox"/> Employee Identification Number	<input type="checkbox"/> Taxpayer Identification Number
<input type="checkbox"/> Professional License Number	<input type="checkbox"/> Legal Entity Identifier
<input type="checkbox"/> Credit/Debit Card Number	<input type="checkbox"/> National Futures Association ID
<input type="checkbox"/> Personal Bank Account Number	<input type="checkbox"/> Other ID if it can be traced back to an individual
<input type="checkbox"/> Personal Device Identifiers or Serial Numbers	
Contact Information	
<input type="checkbox"/> Personal Mobile Number	<input checked="" type="checkbox"/> Business Phone Number
<input type="checkbox"/> Personal E-mail Address	<input checked="" type="checkbox"/> Business E-mail Address
<input type="checkbox"/> Home Phone Number	<input type="checkbox"/> Personal or Business Fax Number
<input type="checkbox"/> Home Mailing Address	<input checked="" type="checkbox"/> Business Mailing Address
Sole Proprietors	
<input type="checkbox"/> Business Taxpayer Identification Number	<input checked="" type="checkbox"/> Business Mailing Address
<input type="checkbox"/> Business Credit Card Number	<input checked="" type="checkbox"/> Business Phone or Fax Number
<input type="checkbox"/> Business Bank Account Number	<input checked="" type="checkbox"/> Business Mobile Numbers
<input type="checkbox"/> Business Device identifiers or Serial Numbers	
Biographical Information	
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Gender

<input type="checkbox"/> Date of Birth	<input type="checkbox"/> City or County of Birth
<input type="checkbox"/> Country of Birth	<input type="checkbox"/> Zip Code
<input type="checkbox"/> Citizenship	<input type="checkbox"/> Military Service Information
<input type="checkbox"/> Spouse Information	<input type="checkbox"/> Academic Transcript
<input type="checkbox"/> Group/Org. Membership	<input type="checkbox"/> Resume or Curriculum Vitae
<input type="checkbox"/> Location Data (e.g., GPS)	<input type="checkbox"/> Nationality
<input type="checkbox"/> Employment Information	<input type="checkbox"/> Marital Status
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Children Information
Biometrics/Distinguishing Features/Characteristics	
<input type="checkbox"/> Fingerprints	<input type="checkbox"/> Height
<input type="checkbox"/> Retina/Iris Scans	<input type="checkbox"/> Voice/Audio Recording
<input type="checkbox"/> Hair Color	<input type="checkbox"/> Eye Color
<input type="checkbox"/> Video Recording	<input checked="" type="checkbox"/> Photos (may be included in a presentation submission)
<input type="checkbox"/> Weight	<input type="checkbox"/> Signatures
Active Directory/Device Information	
<input type="checkbox"/> IP Address	<input type="checkbox"/> MAC Address
<input type="checkbox"/> CFTC Asset Number	<input type="checkbox"/> Device Identifiers or Serial Numbers
<input type="checkbox"/> User Name	

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

To effectively implement and manage these components, the CFTC must be able to communicate with the innovator community. To accomplish this task, CFTC has implemented a secure website portal including a collection form, and dedicated email address to facilitate communications with the FinTech community.

The collection form includes fields to collect contact information allowing CFTC to respond to the submitter and provide feedback and coordinate subsequent communications. The form also includes a free text field and the ability to upload files.

The CFTC email system resides on the CFTC General Support System (GSS), which has its own PIA. The CFTC email system is continuously monitored for operational and security risks by CFTC Office of Data Technology (ODT). Access to the LabCFTC mailbox is restricted to CFTC personnel who have a need to know the information.

2) If any forms are used to collect information that resides in the system, please include the name of such form(s) and any applicable control number.

Form	Control No. (If applicable)
LabCFTC Office Hours Web Form	

V. INFORMATION USE

- 1) Will information in the system be retrieved using one or more of the data elements listed in Section III?

Yes, information in the system can be retrieved by name.

- 2) If the information in the system is retrieved using one or more of the identifiers, what CFTC System of Records Notice (SORN) covers the information?

Yes, the Privacy Act records maintained in this system are covered by CFTC-50, LabCFTC.

VI. ACCESS AND SHARING

- 1) With which internal CFTC Offices or Divisions is the information shared? For each Office or Division, what information is shared and for what purpose?

The information collected and maintained by LabCFTC may be shared with other CFTC Offices or Divisions including Commissioners offices, Division of Clearing and Risk, Division of Market Oversight, Division of Swap Dealer and Intermediary Oversight, Office of the Chief Economist, and Office of International Affairs. The information is shared to facilitate dialogue between innovators and those within the CFTC on financial and technological innovations and to educate internal and external stakeholders on how financial technology innovations are being used in the financial markets.

- 2) How is the information shared internally?

The information is shared internally either through email, SharePoint, or by saving it on the LabCFTC share drive with access limited only to LabCFTC staff.

- 3) With which external organization(s) is the information shared?

For CFTC hosted competitions under the AICA, winners' names and company information may be posted publicly on CFTC.gov. Other than competitions, LabCFTC has not historically shared information outside of the CFTC.

- 4) How is the information shared externally?

Historically, LabCFTC has not shared information externally. If future sharing is contemplated or required, LabCFTC, when feasible, will provide appropriate notice and the data will be transferred in a manner designed to prevent the unnecessary and/or unauthorized disclosure of sensitive information.

VII. TRANSPARENCY

- 1) How are individuals notified as to how their information will be collected, used, and/or shared within this system?

Notice to individuals is provided by this PIA as well the applicable SORN. In addition, the Commission's website Privacy Policy describes what information is collected and stored automatically when individuals visit the Commission's website. When CFTC hosts competitions under the AICA, a competition-specific privacy notice is included on the competition announcement.

- 2) Is a SORN is required? If so, explain how the use of the information in this system is limited to the use specified in the SORN?

Yes, a SORN is required. LabCFTC information is covered under CFTC-50, *LabCFTC*. The use of the information is limited to the use specified in the SORN by limiting access to the information to LabCFTC staff who understand the uses in the SORN as well as the uses described in the PIA.

VIII. INDIVIDUAL PARTICIPATION

- 1) Is the information collected directly from the individual?

Information is collected directly from the individuals who choose to complete the web form, submit an email to LabCFTC's dedicated inbox, or attend CFTC in-person office hours. Information about individuals is also collected indirectly when it's provided on behalf of meeting attendees or competition submissions by company representatives who are responsible for scheduling appointments or are otherwise authorized to provide information on their behalf.

- 2) Is the collection mandatory or voluntary? If voluntary, what opportunities do the individuals have to decline to provide information?

All personal information collected by LabCFTC is submitted voluntarily. Individuals determine how much information to provide.

- 3) Do individuals have an opportunity to consent to a particular use of the information? If so, how do they provide consent for a particular use?

For CFTC hosted competitions under the AICA, participants and winners have an opportunity to consent to their information being posted publically on CFTC.gov.

IX. DATA MINIMIZATION

- 1) What steps were taken to minimize the collection of PII in the system?

The system collects the minimum amount of contact information necessary to follow up with requests and inquiries and to facilitate LabCFTC competitions. LabCFTC staff worked closely with the Privacy Office when developing the LabCFTC Office Hours Web Form and the competition registration requirements to ensure that only the minimum amount of PII necessary is collected.

X. DATA QUALITY AND INTEGRITY

- 1) How is data quality ensured throughout the information lifecycle and business processes associated with the use of the information?

- Cross referencing data entries with other systems
- Third party data verification
- Data taken directly from individuals
- Character limits on text submissions
- Numerical restrictions in text boxes
- Other:

XI. RETENTION

- 1) What are the retention periods for the information?

The records will be maintained in electronic form. Data that is initially collected and stored on the AWS platform will only be stored on the AWS platform until the data is transferred to the internal CFTC backend systems. Once the data transfer is verified, the data stored on the AWS platform will be purged. The data stored on the backend CFTC systems will be maintained in accordance with the External Outreach – Education, Awareness, and Innovation records schedule, which requires that records be closed at the end of the calendar year and then destroyed seven years after closed. The disposition authority number is DAA- 0180-2018-0007-0002.

XII. SECURITY

- 1) What types of administrative safeguards protect the information?

- Contingency Plan
- User manuals for the system
- Rules of Behavior
- Non-Disclosure or other contractual agreement
- Other:

2) What types of physical safeguards protect the information?

- Guards
- Identification Badges
- Biometric
- Cameras
- Physically secured space with need to know access
- Other: LabCFTC does on occasion host LabCFTC office hours in non-CFTC managed facilities. LabCFTC staff who participate in the office hours are responsible for safeguarding materials received on such occasions until they are safely returned to a CFTC office location where they are appropriately stored and filed.

3) What types of technical safeguards protect the information?

- User Identification
- Firewall
- Virtual Private Network (VPN)
- Multi-factor Authentication (MFA)
- Passwords
- Encryption
- De-Identification
- Anonymization
- Other:

4) What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate use of the information?

Internal systems such as email servers, SharePoint and network drives are continuously monitored to detect unauthorized access as part of CFTC's security program. Access is limited to those with a need to know who understand their responsibilities in handling this information to prevent inappropriate use of the information.

5) Is this system hosted by a Cloud Service Provider (CSP)? Yes (LabCFTC Web Form)

- a. If yes, which one? Amazon Web Services Commercial Cloud
- b. If yes, has the system obtained a FedRAMP Authorization? Yes.

XIII. TRAINING

1) What privacy training is provided to users of the system?

All CFTC personnel are subject to CFTC agency-wide procedures for safeguarding PII and receive annual privacy and security training.