

Privacy Threshold Analysis (PTA)  
and/or Privacy Impact Assessment (PIA)

for

Division of Depositor and Consumer Protection (DCP) use of  
Enterprise Public Inquiry and Complaints (EPIC) on the Salesforce  
Platform



Date Approved by Chief Privacy Officer (CPO)/Designee: 12/19/2017

## SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

### 1. Describe the outsourced service and its purpose.

The Enterprise Public Inquiry and Complaints (EPIC) effort will be an enterprise Software as a Service (SaaS) solution that is built on the Salesforce platform. It will be a configured solution to manage public and banker complaints and inquiries received by the Federal Deposit Insurance Corporation (FDIC). EPIC is an automated, online system that enables staff within the Division of Consumer Protection (DCP) to add, update, review, and report on individual cases of consumer and financial institution complaints and inquiries. The methods of communication to be managed within EPIC include complaints and inquiries received via telephone, email, web-forms, mail, and fax.

EPIC captures regular and controlled correspondence and telephone calls from consumers and financial institutions that are not examination related. EPIC is a nationwide system that is accessible from FDIC's Washington, Regional, and Field Offices. In addition to full data entry capabilities, users can print reports based on user-specified criteria, attach scanned documents to specific records, and automatically generate reply letters.

The solution will be acquired and delivered in phases. The initial 2017 scope of work involves the replacement of two legacy systems used for two communication and inquiry tracking systems:

*-Office of the Ombudsman's Communication Tracking System - Ombudsman Automated Tracking System (CTS-OATS); and*

*-DCP's Specialized Tracking and Reporting System (STARS).*

DOA's Customer Communication and Tracking System (CCATS) will be replaced in 2018.

## SECTION II – DATA TYPE, SOURCES, AND USE

### 2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

#### **DCP in EPIC**

DCP, through EPIC, receives, responds to, tracks, and reports on complaints and inquiries received from the public and bankers. The three divisions that receive these complaints and inquiries, namely the Division of Administration (DOA), Division of Insurance and Research (DIR) and Division of Consumer Protection (DCP), will need to be able to store information related to the communications and report to a variety of constituencies on the complaints and inquiries they receive and process. Hence, all communications made to the FDIC by the customer(s) must be tracked within the EPIC system. The categories of customers who may contact these divisions are: Consumer, Academia, Banker, Analyst, Congress/Senate/White House, Media/Press, Attorney,

Professionals, FDIC-Management, FDIC-Employee, and other Federal, State and Local Agencies. EPIC will store personally identifiable information (PII) for DCP use. PII will be collected via incoming calls to the FDIC, mail, email, fax, and online forms.

The Customer Assistance Form (CAF) is used by the public to submit their complaints or inquiries regarding various banking issues and deposit insurance. Once the consumer completes the form and submits their request, the form's programming will pass the data to EPIC. A record is created, and the incoming CAF submission is attached to the record. The forms collect: Requestor Type (e.g., academic, banker, consumer), Name, Email address, Phone/Fax numbers, Title, Organization name, State, and Question. Also, if applicable, the form collects previously contacted FDIC Information and the Financial Institution's Name, City, State, and Cert. Only Name, Email address, and question are mandatory as they are deemed necessary to answer the request. The other fields are optional and are collected in order to better serve the requestor.

Correspondence can be received from consumers via the online Customer Assistance Form (CAF) or email which is reviewed and then saved to EPIC. Correspondence is also received through the U.S. Mail or via fax, which are then scanned to create an electronic image and subsequently linked to an EPIC record. Telephone calls received directly by the Consumer Response Center (CRC) or from the FDIC Call Center that require a CRC subject matter expert, are also entered into EPIC.

EPIC contains the complainant's incoming correspondence, internal codes to identify the complainant's concerns, information concerning the bank in question (bank name, address, class code, supervisory region), and internal tracking dates regarding action(s) taken on the record.

EPIC contains consumer correspondence that may have been referred from another federal regulatory agency. For example, if a consumer writes to the Office of the Comptroller of the Currency (OCC) about a financial institution supervised by FDIC, the OCC would forward the incoming consumer correspondence to the FDIC for handling and responding.

EPIC may also contain consumer correspondence that was referred from another state banking agency.

EPIC will also store FDIC employee names to assign user profiles (giving some administrative access and others standard user access) in EPIC. This is to allow FDIC to manage which EPIC users are managing which complaints. EPIC does not have any fixed database fields to record PII (SSN, personal bank account or financial information, date of birth, etc.) However, the users of EPIC are tasked with imaging incoming paper correspondence and attaching emails or input from the CAF into EPIC. While correspondents with the FDIC are never asked to submit this PII, there is no way to prevent a submitter from including any type of data in the correspondence. Although the consumer can not opt-out of providing the PII which is needed to respond back to the requestor (name, address, email, etc.), the requestor can indicate in the incoming correspondence that they do not want their correspondence shared with anyone outside the FDIC, (i.e., with the financial institution in question). Any additional PII identified by FDIC staff that is not necessary to respond to the complaint (not one of the identified PII elements in question 4) will be redacted prior to input into EPIC and/or deleted from EPIC upon discovery.

**3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.**

DCP, through EPIC, receives, responds to, tracks, and reports on complaints and inquiries received from the public and bankers. The three divisions that receive these complaints and inquiries, namely DOA, DIR and DCP, will need to be able to store information related to these communications and report to a variety of constituencies on the complaints and inquiries they receive and process. Hence, all communications made to the FDIC by the customer(s) must be tracked within EPIC. The categories of customers who may contact these divisions are: Consumer, Academia, Banker, Analyst, Congress/Senate/White House, Media/Press, Attorney, Professionals, FDIC-Management, FDIC-Employee, and other Federal, State and Local Agencies. The PII collected is both relevant and necessary for the purpose for which it was designed. This is part of the system design and is documented in the EPIC user manual. Data can be retrieved by the complainant's name, address, email address, or telephone number. Management reports are used to monitor workflows or timeliness. Authorized users may access reports and distribute them to internal, first-line supervisors. Supervisory records are kept logically separated in the EPIC solution.

**4. What types of personally identifiable information (PII) are (or may be) included in the information specified above?**

The only PII that EPIC maintains for DCP is the full name of the DCP user and the below PII of the complainant. Any of the following may be collected through open text fields in the online comment form or included by the complainant in their complaint submission, but will be removed by DCP staff when identified.

PII Element	Yes	No
Full Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Date of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Place of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Social Security Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Employment Status, History or Information ( <i>Organization Name and Title</i> )	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mother's Maiden Name	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Home Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Phone Number(s) (non-work)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email Address (non-work)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee Identification Number (EIN)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Driver's License/State Identification Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vehicle Identifiers (e.g., license plates)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Education Records	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Criminal Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Military Status and/or Records	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Investigation Report or Database	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Biometric Identifiers (e.g., fingerprint, voiceprint)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Photographic Identifiers (e.g., image, x-ray, video)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other (Specify: _____)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

- a) Explain the business purpose requiring the collection of SSNs: N/A
- b) Provide the legal authority which permits the collection of SSNs. N/A
- c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: N/A

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 <input type="checkbox"/>	1-500 <input type="checkbox"/>	501-1,000 <input type="checkbox"/>	1,001 - 2,500 <input type="checkbox"/>	2,501 - 5,000 <input type="checkbox"/>
5,001 - 7,500 <input type="checkbox"/>	7,501 - 10,000 <input type="checkbox"/>	10,000 - 50,000 <input checked="" type="checkbox"/>	50,000 - 100,000 <input type="checkbox"/>	over 100,000 <input type="checkbox"/>

6b. If "0" was answered for 6a, please explain<sup>1</sup>: N/A

7. What are the sources of data (both PII and non-PII) for the outsourced service/project? How is the data derived?

Data Source <sup>2</sup> (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	Type of Data Provided by Source & How It is Derived (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	Does Data Include PII?
FDIC Consumer Response Center (CRC) and FDIC Call Center	Individuals calling the FDIC about a complaint or inquiry will speak with the CRC or Call Center, who may collect PII so EPIC users can correspond with the individual. This may include any of the PII specified in question 4.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
U.S.P.S. Mail	Individuals who send postal mail about a complaint or inquiry may send any of the PII specified in question 4.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Email	Individuals who send email about a complaint or inquiry may send any of the PII specified in question 4.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Fax	Individuals who send a fax about a complaint or inquiry may send any of the PII specified in question 4.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Customer Assistance Form (CAF) (Online at FDIC.gov)	Individuals who fill out the CAF on FDIC.gov about a complaint or inquiry may include any of the PII specified in question 4. This will automatically send the information to EPIC.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
FDIC Personnel	DCP personnel will manually enter CRC and Call Center complaint data and any scanned documents/images sent via U.S.P.S. mail, email or fax associated with the complaint to EPIC; DIT personnel will enter OO users' full name in the EPIC system for account creation and management.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

<sup>2</sup> Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

CALL Report Data from System of Uniform Reporting of Compliance and CRA Examinations (SOURCE)	CALL Report Data (from SOURCE System) provides basic bank asset information to EPIC (regarding the bank identified by the complainant to EPIC).	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Structure Information Management System (SIMS)	SIMS provides basic bank structure bank data to EPIC (e.g., Bank name, HQ address, asset size, web URL, FDIC Cert. number, etc).	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
FDICConnect (FCX)	FCX provides data to EPIC. Regulated banks, via FCX, can share responses to complaints, including PII information about complainants (which include any/all of the PII from question 4).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

**8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?**

Yes, data can be retrieved by a personal identifier – complainant’s name, address, email address, or telephone number.

**9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.**

EPIC operates under the FDIC Privacy Act SORN 30-64-0005, *Consumer Complaint and Inquiry Records* (80 FR 66987).



**This completes the PTA.**

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 2 and NO for all items in question 4; OR
  - Only Full Name in question 4.
  
- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 thru 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.
  
- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office ([privacy@fdic.gov](mailto:privacy@fdic.gov)).

## SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that the Outsourced Service Provider will share or provide PII data to as part of the outsourced service.

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<i>N/A – no Salesforce staff will have access to any PII contained within EPIC.</i>
10b. FDIC Personnel and/or FDIC Systems/ Applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>PERSONNEL</b> DCP, DIR, and DOA employees will have access to the PII within EPIC in the course of their work (while managing cases and communicating within EPIC). This may include some or all of the PII specified in question 4.</p> <p><b>SYSTEMS</b> EPIC shares data to the Data Gathering Tool (DGT) to provide complaint information to bank examination staff. This allows bank examination staff to have a general idea of the volume/type of complaints against a bank when an examination commences.</p> <p>EPIC is integrated to Microsoft Outlook 365. DCP users of EPIC send an “FDIC basic acknowledgment” email to complainants upon receipt of the complaint or inquiry. EPIC will share the complainant’s email address with Outlook for this purpose. Additionally, Outlook is used to communicate with external banking agencies about a complaint, secured via Zix.</p> <p>EPIC is integrated to the Extranet (to allow one way communication from EPIC to State Banking Authorities); DCP users of EPIC, once an MOU is executed, share complaints about the financial institutions regulated by the respective states. EPIC could share PII of complainants (which include any/all of the PII from question 4).</p> <p>EPIC is integrated to FCX (to allow 2 way communication with regulated banks). DCP users of EPIC share complaints to regulated banks, including PII of complainants (which include any/all of the PII from question 4).</p> <p>EPIC is integrated to DCP’s Quarterly Compliance Risk Profile Tool. This is summary data (volume of complaints per bank, etc.).</p>



			<p>FDIC CONTRACTORS</p> <p>FDIC Salesforce Integrator support contractors will have access to PII within EPIC to build and support the EPIC solution to meet FDIC specifications.</p>
<p><b>10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<p><i>N/A – no members of the public will have access to any PII contained within EPIC.</i></p>
<p><b>10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>EPIC, through FDICconnect, may share complaint/inquiry correspondence with federally regulated banks. This may include any of the PII that was specified in question 4.</p>
<p><b>10e. Federal, State, and/or Local Agencies</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>EPIC, through Outlook (secured by Zix), may share complaint/inquiry correspondence with other financial regulatory agencies (e.g., the Federal Reserve, Consumer Financial Protection Bureau, and the Office of the Comptroller of the Currency). This may include any of the PII that was specified in question 4. If a consumer's incoming correspondence is sent to another federal regulatory agency for handling, the consumer is sent a letter notifying them of the referral and providing them the name and address of the agency.</p> <p>EPIC, through the Extranet, may share complaint/inquiry correspondence with state banking authorities. This may include any of the PII that was specified in question 4.</p>
<p><b>10f. Other</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<p><i>N/A</i></p>

**11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?**

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FDIC Confidentiality Agreement (Individual)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Non-Disclosure Agreement (NDA)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Memoranda of Understanding (MOU)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Information Sharing Agreements (ISA)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication Risk Assessment	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other Applicable Agreement(s) (Specify: _____)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<p><b>If you answered NO to any item above, please provide additional information if available: _____</b></p>		

**SECTION IV – NOTICE AND CONSENT**

**12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?**

No. Individuals do not have the opportunity to “opt out” of providing their data and/or consenting to particular uses of their information.

Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information.

Customers initiate contact with FDIC by submitting either inquiries, requests, complaints (regarding financial institutions), and/or suggestions. At any point during this process, the customer can choose to remain anonymous and opt-out of providing any PII. However, if they would like to receive a written response from the FDIC, they must provide the necessary PII so that FDIC may mail/email them a response.

**13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?**

No

Yes *(If yes, check applicable box(es) below.)*

- Link to FDIC Privacy Policy
- FDIC Privacy Act Statement
- Contractor Privacy Policy or Statement
- No Privacy Policy has been posted

**SECTION V – DATA SECURITY AND ACCURACY**

**14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider’s care.**

[Outsourced Information Service Provider name] [has gone/will go] through the security review required by the FDIC’s Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved?  NO  YES

The FDIC conducts background investigations (BIs) on key Salesforce personnel and other applicable personnel prior to their beginning work on the contract.

Salesforce is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsourced Service

Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements. As per the FedRamp Package.

Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) **Attach the Contract Clause Verification Checklist to the back of this form.**

Appropos to FedRamp-certified PAAS solutions, Salesforce has not gone through the FDIC Information Service Provider Assessment Methodology. Salesforce has gone through the FedRamp Certification process. FDIC has reviewed this package. The Salesforce Platform is going through the FDIC ATO process.

EPIC user account creation and deletion requests go through the FDIC standard access control procedures, which require management approval, as well as setting up the internal user profiles through the applications administrative table. Users' rights are limited by role.

Users only have access to EPIC data pertaining to records they are authorized to access (for example, those with access to telephone records only, do not have access to stored images of correspondence).

Complaint and inquiry data is available to other federal regulatory agencies upon request. These requests may involve the volume of complaints and inquiries that were received for a specific timeframe, or may be based on the subject of the complaint, (ie., number of credit card complaints received). Senior Management determines the criteria for the type of data shared and no agreements have been effected.

Authorized users are responsible for properly using the data and are accountable if the data is compromised.

**15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date?**

Data is collected directly from individuals. As such, the FDIC and its vendors rely on the individuals to provide accurate data.

The vendor/contractor works with FDIC to verify the integrity of the data [before, in conjunction with, and/or after] inputting it into the system or using it to support the project.

As necessary, an authorized user of EPIC checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

Other (*Please explain.*)

Data-integrity checks are completed against required fields to ensure FDIC has the data needed to provide a response back to the complainant.

**16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider.**

Within FDIC, the Enterprise Public Inquiry and Complaints (EPIC) Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated personnel to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data.

The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

None of the above.

## **SECTION VI – DATA RETENTION AND DISPOSAL**

**17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.**

The EPIC system is only operated in the Salesforce Gov Cloud. In May 2014, Salesforce achieved and has since maintained a FedRAMP Agency Authority to Operate (ATO) at the moderate impact level issued by U.S. Department of Health and Human Services (HHS) for the Salesforce Government Cloud.

**18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.**

The retention period is seven years from the record closed date, which is in accordance with the FDIC's Records Management Policy. Hardcopy files are deleted by shredding and the electronic files

are deleted after seven years in accordance with the FDIC's Records Retention and Disposition Schedule.

Hardcopy documents are maintained while the complaint is open for reference purposes, and are shredded after the complaint is closed (this is generally completed within 60 days, except for Fair Lending cases, which may take up to 180 days).