



# FARM CREDIT ADMINISTRATION

## PRIVACY IMPACT ASSESSMENT

### SYSTEM, PROGRAM, OR PROJECT NAME

Criminal Referral System

### SYSTEM TYPE

Information Technology System or Capability

### PURPOSE

As the regulator of the Farm Credit System (FCS or System), the Farm Credit Administration receives copies of reports of known or suspected criminal activity from System institutions in accordance with the agency's published regulations on criminal referrals.

### AUTHORITY

12 U.S.C. 2243, 2252, 2254; 12 CFR part 612 subpart A (§§ 612.2130 – 612.2270) and subpart B (§§ 612.2130 – 612.2270)

### INFORMATION OVERVIEW

Covered Persons	Included
Farm Credit institution employees	<input checked="" type="checkbox"/>
Farm Credit institution customers	<input checked="" type="checkbox"/>
FCA employees, contractors, interns	<input checked="" type="checkbox"/>
Employees of other federal agencies	<input checked="" type="checkbox"/>
Members of the public	<input checked="" type="checkbox"/>

Personally Identifiable Information (PII) Element(s)	Included
Full name	<input checked="" type="checkbox"/>
Date of birth	<input checked="" type="checkbox"/>
Place of birth	<input type="checkbox"/>
Social Security number (SSN)	<input checked="" type="checkbox"/>
Employment status, history, or information	<input checked="" type="checkbox"/>
Mother's maiden name	<input type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage)	<input type="checkbox"/>
Medical information (medical record numbers, medical notes, or X-rays)	<input type="checkbox"/>
Home address	<input checked="" type="checkbox"/>
Phone number(s) (nonwork)	<input checked="" type="checkbox"/>
Email address (nonwork)	<input checked="" type="checkbox"/>
Employee identification number (EIN)	<input checked="" type="checkbox"/>
Financial information	<input checked="" type="checkbox"/>
Driver's license/State identification number	<input checked="" type="checkbox"/>
Vehicle identifiers (e.g., license plates)	<input checked="" type="checkbox"/>
Legal documents, records, or notes (e.g., divorce decree, criminal records)	<input checked="" type="checkbox"/>
Education records	<input type="checkbox"/>

Personally Identifiable Information (PII) Element(s)	Included
Criminal information	<input checked="" type="checkbox"/>
Military status and/or records	<input type="checkbox"/>
Investigative report or database	<input type="checkbox"/>
Biometric identifiers (e.g., fingerprint, voiceprint)	<input type="checkbox"/>
Photographic identifiers (e.g., image, X-ray, video)	<input type="checkbox"/>
Other (specify): System-generated criminal referral number, system administrative data (audit and use information for FCS and FCA users)	<input checked="" type="checkbox"/>

## LIFE CYCLE NARRATIVE

FCA regulations (12 CFR part 612, subpart B) require FCS institutions to report known or suspected criminal activity involving FCS institutions. The agency uses these referrals to assist in safety and soundness examinations of System institutions and to provide information to federal law enforcement authorities.

FCA provides a secure web form to authorized users at each System institution on an external data portal. These users log in to the external data portal with their existing credentials. On the portal, they can create new criminal referrals and access existing criminal referral forms. Existing referrals include both previously submitted referrals and those pending submission. For submitted referrals, a date and time of submission and a referral number are provided. For pending submissions, only a creation date and time appear.

Information entered on the web form is temporarily housed in the user's browser and is purged upon submission to FCA, except for the date and time of submission and a system-generated referral number. Unfinished or unsubmitted forms are automatically deleted from a user's system after 60 days. Because the web form relies on local browser storage and cannot be transferred or retrieved across systems, a user must log in to the FCA external data portal to access an unsubmitted web form on the same computer and browser he or she used to create the web form.

Users can generate PDF copies of their submissions, which they can submit to the appropriate law enforcement authorities as required by regulation. After submission, users may not access any PII included in the submission, revise or edit the submission, or generate a new PDF copy of the submission. All data, including PII, are encrypted at all times — that is while stored on the user's system, in FCA's database, and in transit between the user's machine and FCA.

Once the form has been submitted, FCA performs data validation on the criminal referral data and then places these data in an encrypted database. This encrypted database delivers certain information in the criminal referral to internal FCA users who have a need to know in support of their duties, via an internal, custom application. The application is part of a suite of tools hosted in the agency's general support system (GSS), which FCA staff in the Office of Examination (OE) and the Office of General Counsel (OGC) use to conduct supervisory, examination, and enforcement activity. Access is via single sign-on authentication.

In general, only specific employees in OE and OGC can access criminal referral information. Only certain fields of information in the referral are provided to all authorized users. Other fields, such as the referral subject's name, SSN, and date of birth, are restricted to a limited subset of authorized users on a need-to-know basis. For example, OGC personnel may need detailed information to assist with legal actions, and examiners-in-charge or other senior OE officials may need detailed information as part of their examination and oversight duties. In general, OE examiners who access the criminal referrals database in support of their safety and soundness review duties are limited to viewing the name of the institution and details of the suspected criminal activity. Access to specific names or additional information about a referral may be on a case-by-case basis in coordination with OE and OGC. Most users have read-only access and cannot modify submissions. Certain users in OE and OGC may upload documents or input information into the system to update an existing submitted referral, create a new referral on behalf of an FCS institution, or apply certain metadata about types or categories of referrals to facilitate examination efforts. Access to applications that leverage criminal referral data is limited only to internal users on FCA-issued equipment on a need-to-know basis. The chief examiner and

general counsel are responsible for approving access and for alerting the Office of Information Technology (OIT) when access to these applications and information should be terminated.

Information in the system may be shared internally to facilitate the agency's efforts to ensure the safety and soundness of the FCS and externally in accordance with the routine uses identified in the applicable system of records notice (SORN) FCA-10 – Farm Credit System Institution Criminal Referrals – FCA. Any external sharing of information must be within the scope of the agency's authorities and regulations and facilitate a specific FCA business function. In accordance with the applicable records schedule, records are purged from FCA's system after 15 years.

Information in the criminal referral form is collected from employees of FCS institutions and not directly from persons who are the subjects of referrals. Users who submit information are also required to attest that the information submitted is true and accurate to the best of their knowledge. Persons to whom the information pertains will not receive notice at the time of collection. FCA has published this privacy impact assessment (PIA) and the applicable SORN to mitigate the risk related to notice and consent.

Information provided includes PII about submitters and the individual who is the subject of the referral. PII about submitters includes names, titles, and contact information for their System institutions, such as email addresses and phone numbers. Information about the person who is the subject of a criminal referral includes the following:

- Name and other identifying information, such as date of birth, SSN, tax identification number, or employee identification number
- Information related to financial transactions and other financial information related to the suspected criminal activity
- Contact information, such as mailing address, phone number, and email address
- Employment information, including title, position, and employer
- Information about the referred person's relationship with an FCS institution
- Information about existing actions being taken against the person or previous referrals
- Names of individuals believed to be involved in the criminal activity
- Details of the alleged criminal violation
- Any other supplemental information deemed necessary by the submitter and included as part of the referral

The web form is structured to reduce the amount of unnecessary PII collected — in general, explicit fields for specific data points are included, such as SSN and date of birth. Some free text fields, such as the description of suspected activity, are included. Data validations occur for fields requiring dates and other numbers to ensure data are entered in a correct, standardized format. Users may not upload separate or additional documents through the external data portal.

Individuals who are the subject of the referral may have limited opportunities to access, change, or update information included in the system in accordance with the Privacy Act and FCA's Privacy Act regulations, as outlined in [12 CFR part 603](#).

## COMPLIANCE WITH APPLICABLE STATUTES, REGULATIONS, AND REQUIREMENTS

For each, indicate as applicable and provide a link, or a brief description of compliance. If not applicable, indicate with N/A.

The Privacy Act of 1974 (As Amended)	
System of records notice(s)	FCA's criminal referral system is covered by the Privacy Act system of records: FCA-10 – Criminal Referrals – FCA, available at <a href="#">85 FR 31497</a> .
Computer Matching and Privacy Protection Act of 1980	
Notice of computer matching agreement(s)	N/A — FCA does not have any computer matching agreements that pertain to this system.
The Paperwork Reduction Act of 1995	
OMB control number(s) or related form(s)	N/A — FCA does not have any OMB control numbers or forms associated with this system.
The Federal Records Act of 1950 (As Amended)	
Record(s) control schedule name(s) and number(s)	Records are maintained in accordance with FCA's comprehensive records schedule and the National Archives and Records Administration's general records schedule. Specifically, such items are to be destroyed after 15 years, with longer retention authorized as necessary for business use.
Other	
N/A	N/A

## ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS

<input checked="" type="checkbox"/>	All applicable controls for protecting PII as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Appendix J, and NIST SP 800-122 have been implemented and are functioning as intended, have compensating controls in place to mitigate residual risk, or have an approved plan of action and milestones.
<input checked="" type="checkbox"/>	The system has been reviewed for and assigned a categorization level in accordance with NIST Federal Information Processing Standards (FIPS) Publication 199 and NIST SP 800-60, and the senior agency official for privacy has approved the categorization. FIPS 199 Security Impact Category: <u>Moderate</u>
<input checked="" type="checkbox"/>	A security assessment has been conducted for the system, and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	The information system has been secured in accordance with Federal Information Security Modernization Act requirements. Most recent assessment and authorization type: Authorization to Use (ATU) and Date: <u>8/6/2019</u> <input type="checkbox"/> This is a new system, and the assessment and authorization date is pending.
<input checked="" type="checkbox"/>	A comprehensive listing of data elements included in the system has been provided to the privacy officer, reviewed and approved, and included in the agencywide PII inventory.
<input checked="" type="checkbox"/>	System users are subject to or have signed confidentiality or nondisclosure agreements as applicable.
<input checked="" type="checkbox"/>	System users are subject to background checks or investigations.* *FCA employees undergo background checks.
<input checked="" type="checkbox"/>	System access is limited to authorized personnel with a bona fide need to know in support of their duties.
<input type="checkbox"/>	Notice is provided in the form of a Privacy Act statement, privacy notice, privacy policy, or similar, as applicable.
<input type="checkbox"/>	Contract(s) or agreement(s) (e.g., memorandums of understanding, memorandums of agreement, and information security agreements) establish ownership rights over data, including PII.
<input type="checkbox"/>	Acceptance of liability and responsibilities for exposure of PII are clearly defined in agreement(s) or contract(s).
<input checked="" type="checkbox"/>	Access to and use of PII are monitored, tracked, and recorded.
<input checked="" type="checkbox"/>	Training on PII, confidentiality, and information security policies and practices is provided to system users or those with access to information.

## ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS NARRATIVE

FCA's criminal referral system consists of an access-restricted web form on the agency's website (fca.gov) and an internal database, which delivers submitted criminal referral information to an internal custom application. As described above, access to the web form is limited, and unfinished and unsubmitted forms are deleted after 60 days; during that time, the authorized user's browser securely stores the data entered on the form before submission and transmission to FCA. The FCA database server, which receives, stores, and delivers criminal referral information, and the custom application through which internal users access the information, are part of the agency's GSS.

FCA's GSS is categorized as a moderate system, and FCA's chief information officer (CIO) has granted the system an ATU. The agency secures information in the system using a variety of means, including the following:

- Physical security controls of FCA facilities and data centers that house GSS components
- Use of firewalls, intrusion detection and prevention systems and antivirus and other software and capabilities for detection of malware and other malicious threats
- Use of transport layer security connections and multifactor authentication
- Use of total disk encryption and other encryption methods for securing sensitive data, including PII
- Access controls and use of the principle of least privilege
- Application, network, server, and database activity logs, which are reviewed upon detection of abnormalities or upon request by the CIO or Chief Information Security Officer (CISO).

There are only three types of users:

- *Authorized users of the external data portal:* Generally referred to as "submitters," these individuals have been identified by FCS institutions as responsible for creating and submitting criminal referral forms.
- *Authorized users of the database and custom internal criminal referral application:* These are FCA employees within OGC and OE with a need to know in support of their duties related to examining FCS institutions and enforcing FCA regulations related to suspected criminal activity.
- *Administrators and OIT staff:* These are FCA staff responsible for managing both the external data portal and the agency's custom application.

Annual access and permission reviews of the internal criminal referral application and the accompanying database are carried out by Office of Information Technology staff in coordination with representatives from OE and OGC.

The database that houses criminal referrals is encrypted to ensure PII is protected at rest. Data are also encrypted in the user's browser when the user is creating the referral and when they are in transit between the user's browser and FCA's internal database that houses referrals.

Formalized, documented procedures exist for routing of, access to, and use of criminal referral information by OE and OGC personnel in support of examination and enforcement duties.

All FCA users receive annual IT security and privacy awareness training and are responsible for reviewing and attesting to the requirements outlined in FCA IT security and personal use policies.

## PRIVACY RISK ANALYSIS

What follows is an overview of the primary risks associated with the criminal referral system and a description of corresponding mitigations put in place by the agency for each.

**Data confidentiality, including access or use by unauthorized users:** The primary risk associated with the criminal referral system is the possibility that sensitive PII could be leaked or exposed, or that persons without a clearly defined need to know could gain access to and use of sensitive PII.

To reduce the risks of data loss, leaks, and unauthorized or unnecessary access and use, FCA uses a variety of technical and administrative controls to limit access to data it stores and processes in the criminal referral system; for more information, see the Administrative and Technological Controls Narrative section of this PIA. FCA developed a custom application to specifically address the issue of need to know for sensitive PII associated with criminal referrals. The criminal referral system replaces a legacy process involving general access to PDF copies of referrals. The new system has a granular access, control-based interface that uses the concept of least privilege to limit a specific user's access to information for which he or she has a valid need to know. Within FCA, unique usernames, passwords, and two-factor authentication are used to control access to the system and data. FCA users are required to complete annual security and privacy training and must sign and abide by FCA's security policies and procedures. External submitters are required to use unique passwords and usernames to access the external data portal and are limited to only submitting and accessing referrals on behalf of their FCS institutions.

**Transparency:** The criminal referral system and the criminal referral process, in general, afford limited opportunities for notice to and consent by individuals whose PII may be collected. In the case of the criminal referral system, information is not collected directly from individuals; rather, PII is provided by the FCS institution personnel submitting the referral. Because information in the system is subject to the Privacy Act, notice of the collection of PII through the criminal referral process is provided by the applicable SORN. FCA also has published this PIA to provide additional notice of the collection and use of PII in the criminal referral system.

**Data minimization:** FCA reviews data collections to limit the collection and maintenance of PII to the minimum amount necessary to fulfill the agency's mission. That said, the agency does collect and retain significant amounts of PII, including sensitive PII, as it relates to criminal referrals — some portion of this information is not used directly by FCA, but rather by other law enforcement agencies to whom FCS institutions must report criminal activity, in accordance with the regulations and instructions provided in the criminal referral form. To mitigate the risk associated with collecting large amounts of sensitive PII, the agency developed the internal user interface application; this application limits users' access to only the PII for which they have a valid need to know in support of their duties. Further, FCA developed a web form to use as few free text fields as possible, instead using dedicated, structured fields to reduce the chance of collecting unnecessary data. Finally, the agency employs the appropriate technical, physical, and administrative controls to ensure the PII it does collect and maintain is secured.

**Overall risk:** FCA recognizes the risk inherent in collecting and processing sensitive PII, both as individual data elements (such as SSNs) and contextually (as it relates to purported illegal activity). Therefore, the agency developed an interface that reduces the overall risks associated with collecting and maintaining this information. The agency put controls in place to limit local storage of and access to sensitive PII, both by FCA staff and by external submitters. In addition, the agency developed a structured web form for intake to reduce the chance of unnecessary PII collection and to improve overall data quality. Finally, the agency took steps to publish two public notices — a SORN and this PIA — to be transparent about the collection and use of PII as it relates to the criminal referral process. The agency intends to continue enhancing the criminal referral system. As new capabilities are developed or authorized for use, this PIA will be revised to account for any new privacy risks and the mitigations established to reduce those risks.

DOCUMENT CONTROL

## Approval

<hr/> Wesley Favel, FCA privacy officer	<hr/> Jeannie Shaffer, CISO
<hr/> Charlie Rawls, general counsel	<hr/> Jerry Golley, CIO and SAOP

## Change Control and Approval History

Version	Date	Change Summary
V 1.0	8/4/2020	Initial Version