

Date of Approval: **February 10, 2021**

PIA ID Number: **5536**

## **SYSTEM DESCRIPTION**

*Enter the full name and acronym for the system, project, application and/or database.*

Pre-Verification Bank API Web Service, N/A

*Is this a new system?*

No

*Is there a PCLIA for this system?*

Yes

*What is the full name, acronym and milestone of the most recent PCLIA?*

This PCLIA supersedes PIAID # 2151 created on 03/14/2017

*What is the approval date of the most recent PCLIA?*

3/14/2017

*Changes that occurred to require this update:*

Expiring PCLIA

*Were there other system changes not listed above?*

No

*What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.*

Wage & Investment/W&I

*Current ELC (Enterprise Life Cycle) Milestones:*

System Deployment/Milestone 5

Operations & Maintenance (i.e. system is currently operational)

*Is this a Federal Information Security Management Act (FISMA) reportable system?*

No

## GENERAL BUSINESS PURPOSE

*What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.*

The system is owned by Green Dot Bank. Green Dot is not a contractor of IRS. The system is a means for federal and state government stakeholders to gain pre-verification information on accounts where monies will be deposited. In the case of IRS tax refunds, Return Integrity & Compliance Services (RICS) will use the system to verify accounts where tax refunds will be deposited. Information returned will include a risk score for the account, if a refund going to the account will be rejected back to IRS and if rejected, the reason why. The benefit to IRS will be to identify suspicious refund activity and take appropriate tax administration action.

## PII DETAILS

*Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?*

Yes

*Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?*

Yes

*What types of tax identification numbers (TIN) apply to this system?*

Social Security Number (SSN)

*List the approved Treasury uses of the SSN:*

Law enforcement and intelligence purposes

*Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).*

The system does not use the entire SSN, it only accepts the last 4 digits of the SSN, which is needed to verify that the correct account is matched to the tax return information.

*Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).*

The system does not use the entire SSN, it only accepts the last 4 digits of the SSN, which is needed to verify that the correct account is matched to the tax return information.

Other Taxpayer Identification Number

*Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?*

Yes

*Specify the PII Elements:*

Name  
Financial Account Numbers  
Tax Account Information

*Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?*

Yes

*Specify the types of SBU from the SBU Types List:*

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

*Are there other types of SBU/PII used in the system?*

No

*Cite the authority for collecting SBU/PII (including SSN if relevant).*

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

*Has the authority been verified with the system owner?*

Yes

## **BUSINESS NEEDS AND ACCURACY**

*Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.*

Green Dot needs specific information to match IRS refund deposit records with the Green Dot account records. IRS needs to be 100% sure that we are inquiring about the correct account, so we want to provide the information Green Dot says they need to be sure. Information requested includes: (Full) Direct Deposit Account Number; Taxpayer First Name; Taxpayer Last Name; Taxpayer Last 4 Digits of Social Security Number; Deposit \$ Amount.

*How is the SBU/PII verified for accuracy, timeliness and completion?*

All returns filed with IRS go through systemic validity checks. If they pass the checks, the return is accepted by IRS. If a return is then selected by RICS as a possible identity theft return or questionable income return, RICS takes steps to authenticate if the taxpayer is the true taxpayer. This program originated as a pilot and was operationalized the subsequent year. The IRS pre-verified refund accounts to assist with tax administration activities on suspicious filed returns. Originally, the IRS shared the data with Green Dot, and subsequently also partnered with H&R Block.

## **PRIVACY ACT AND SYSTEM OF RECORDS**

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

*Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.*

Yes

*Identify the Privacy Act SORN(s) that cover these records.*

IRS 24.030 Customer Account Data Engine Individual Master File

## RESPONSIBLE PARTIES

*Identify the individuals for the following system roles:*

## Official Use Only

## INCOMING PII INTERFACES

*Does the system receive SBU/PII from other systems or agencies?*

Yes

*Does the system receive SBU/PII from IRS files and databases?*

No

*Does the system receive SBU/PII from other federal agency or agencies?*

No

*Does the system receive SBU/PII from State or local agency (-ies)?*

No

*Does the system receive SBU/PII from other sources?*

Yes

*Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).*

Organization Name: Green dot Bank

Transmission Method: Application Programming Interface (API)

ISA/MOU: Yes

*Does the system receive SBU/PII from Taxpayer forms?*

Yes

*Please identify the form number and name:*

Form Number: 1040 Form Name: Form 1040

*Does the system receive SBU/PII from Employee forms (e.g. the I-9)?*

No

## DISSEMINATION OF PII

*Does this system disseminate SBU/PII?*

Yes

*Does this system disseminate SBU/PII to other IRS Systems?*

No

*Does this system disseminate SBU/PII to other Federal agencies?*

No

*Does this system disseminate SBU/PII to State and local agencies?*

No

*Does this system disseminate SBU/PII to IRS or Treasury contractors?*

No

*Does this system disseminate SBU/PII to other Sources?*

Yes

*Identify the other source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).*

Organization Name: Green Dot Bank  
Transmission Method: Application Programming Interface (API)  
ISA/MOU: No

Organization Name: H&R Block  
Transmission Method: API  
ISA/MOU: No

*Identify the authority.*

SORNS Number: IRS 42.021 SORNS Name: Compliance Programs and Projects Files

*Identify the Routine Use in the applicable SORN (or Privacy Act exception).*

Sharing of information is agreed upon by both parties and done in a recurrent agreed upon timeframe for the purpose of the prevention of identity theft and refund tax fraud. SORN procedures are followed as prescribed.

*For what purpose?*

Identity theft protection and refund fraud.

## **PRIVACY SENSITIVE TECHNOLOGY**

*Does this system use social media channels?*

No

*Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?*

No

*Does the system use cloud computing?*

No

*Does this system/application interact with the public?*

No

## **INDIVIDUAL NOTICE AND CONSENT**

*Was/is notice provided to the individual prior to collection of information?*

Yes

*How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?*

Privacy Notice is provided in the form 1040 instructions. "The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations".

*Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?*

No

*Why not?*

"The legal right to ask for information is Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. These sections state that individuals must file a return or statement with IRS for any tax for which they are liable, and response is mandatory. The information is used for the purposes of completing, correcting, or processing a return, figuring tax, and collecting tax, interest and penalties".

*How does the system or business process ensure 'due process' regarding information access, correction and redress?*

Due process is followed as prescribed by SORN.

## **INFORMATION PROTECTION**

*Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).*

IRS Owned and Contractor Operated

*The following people have access to the system with the specified rights:*

*IRS Employees*

Users: Read Write

Managers: Administrator

*IRS Contractor Employees*

Contractor Users: Read Write

Contractor Managers: Read Write

*How is access to SBU/PII determined and by whom?*

Need to know / System Owner

## RECORDS RETENTION SCHEDULE

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?*

Yes

*How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.*

Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, which is the IRS published guidance for security guidelines and other safeguards for protecting returns and return information pursuant to 26 CFR 301.6103(p)(4)-1. RCS 29 Item 47 RCS 29 Item 49 RCS 29 Item 55 RCS 29 Item 85

## SA&A OR ASCA

*Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?*

No

*Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?*

Yes

*Describe the system's audit trail.*

Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, which is the IRS published guidance for security guidelines and other safeguards for protecting returns and return information pursuant to 26 CFR 301.6103(p)(4)-1.

## PRIVACY TESTING

*Does the system require a System Test Plan?*

No

*Please explain why:*

Test plan completed when API was created.

## **SBU DATA USE**

*Does this system use, or plan to use SBU Data in Testing?*

Yes

*Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?*

No

*Explain why not:*

Granted as agreed in the Memorandum of Understanding (MOU) and pursuing Publication 1075 requirements.

## **NUMBER AND CATEGORY OF PII RECORDS**

*Identify the number of individual records in the system for each category:*

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: 100,000 to 1,000,000

Other: No

## **CIVIL LIBERTIES**

*Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?*

No

*Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?*

Yes

*Provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable).*

N/A

*Will this system have the capability to identify, locate, and monitor individuals or groups of people?*

Yes

*Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.*

Only authorized individuals with need to know are given access to the system.

*Does computer matching occur?*

Yes

*Does your matching meet the Privacy Act definition of a matching program?*

Yes

*Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?*

Yes

## **ACCOUNTING OF DISCLOSURES**

*Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?*

Yes

*Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.*

Yes