Privacy Impact Assessment
Of
FedProtect ID Theft Protection Program
(FedProtect Program)

Program or application name:

FedProtect ID Theft Protection Program (FedProtect Program)

System Owner:

Board of Governors of the Federal Reserve System (Board)

Contact information:

System Manager:	Tameika Pope
Title:	Chief Human Capitol Officer
Division:	Management Division
Address:	20th Street and Constitution Avenue, N.W. Washington, DC 20551
Telephone:	(202) 973-7435
IT System Manager:	Jason Zirpoli
Title:	Senior Vice President, Technology
Division:	Office of Employee Benefits of the Federal Reserve System (OEB)
Address:	One Riverfront Plaza 1037 Raymond Blvd, Suite 100 Newark, NJ 07102
Telephone:	(973) 848-3600

Description of the program:

The FedProtect ID Theft Protection Program (FedProtect Program) provides identity theft protection services, which are administered by Allstate Identity Protection. The FedProtect Program is available to all employees of the Board of Governors of the Federal Reserve System (the Board) who take an oath of office and are appointed into

Board service. Coverage is also provided to an employee's eligible dependents, which includes a spouse or domestic partner. Collectively, the covered individuals who are not Board employees are referred to as "family members."[1]

The Board provides support to Allstate Identity Protection through the Office of Employee Benefits of the Federal Reserve System (OEB), by supplying information regarding new Board employees and changes in employment status of existing Board employees. The FedProtect Program offers two levels of services – the Base Benefit and the Additional Benefit.

Employees and their family members are automatically covered by the Base Benefit, which provides coverage for identity theft restoration, up to one million dollars in identity theft insurance, and call-center support. It may still be necessary for the family member to provide information in order to obtain the benefit. It should also be noted that if a family member seeks coverage for an identity theft event with Allstate Identity Protection, the event will be covered under the Base Benefit identity theft insurance policy, even if the event took place before the family member provided his or her information to Allstate Identity Protection.

At their option, Board employees or their family members may also voluntarily register for the Additional Benefit, which requires the provision of additional information. The Additional Benefit consists of optional services, including:

- Identity monitoring – monitors personally identifiable information (PII) to help identify potential misuse.
- Credit monitoring – provides continuous credit monitoring, credit alerts, monthly credit scores, and annual credit reports. **Note**: Family members under the age of 18 are not eligible to register for credit monitoring.
- Financial transaction monitoring – provides alerts when financial limits set by the individual exceed the threshold on accounts and transactions.
- Social media reputation monitoring – provides actionable alerts to help defend from reputational damage or cyberbullying on social media sites.
- Dark web monitoring – monitors and replaces the informational contents of a lost or stolen wallet through a secure database that stores copies of important information located in an individual's wallet. Such information can be monitored for unauthorized use in the dark web, such as the unauthorized use of credit card, phone numbers, medical ID numbers, etc.

1. The information concerning individuals that is being collected and/or maintained are:

Allstate Identity Protection uses an online system to collect and store the information needed to administer the FedProtect Program.

[1] The determination of coverage as an employee family member is determined by whether they would be eligible for coverage under the Federal Employees Health Benefits Program, such as an employee's child.

The Board, through the OEB, provides Allstate Identity Protection the following information to verify that all Board employees are eligible to access the Base Benefit:

- Name;
- Employee ID;
- Employment status;
- Place of employment; and
- Separation date and mailing address (only provided when employee separates from Board employment).

Information (e.g., name, address, or date of birth) about family members is not required to obtain coverage under the Base Benefit. However, in the event of an identity theft incident, this information will be requested by Allstate Identity Protection if it has not been previously provided in order to obtain the benefit.

In addition, at their option, Board employees may choose to register themselves and their family members for the Additional Benefit using Allstate Identity Protection's online system or by phone. In order to register for the Additional Benefit, the individual must provide the following information:

- Mailing address;
- Email address;
- Phone number;
- Date of birth; and
- Social Security Number.

Depending upon the particular Additional Benefit the individual selects, the individual may also have to provide additional information, such as:

- Financial institution credentials (Financial transaction monitoring);
- Social media logins (Social media reputation monitoring);
- Social Security Number (Credit monitoring); and
- Items such as credit card information, driver's licenses, gaming credentials, passports, professional license numbers, Drug Enforcement Agency numbers or insurance card data (Dark web monitoring).

2. Source(s) of each category of information listed in item 1:

The Board generally serves as the source of information collected and maintained for the Base Benefit for employees. In the event an employee or family member experiences identity theft, the employee or family member may need to provide additional information as part of the Base Benefit. The employee or family member serves as the source of information for the Additional Benefit.

3. Purposes for which the information is being collected:

The Board offers identity theft protection services through the FedProtect Program as an employer-paid program to Board employees and their family members to assist them in managing and mitigating the risk associated with identity theft.

4. Who will have access to the information:

Employees or their family members have access to their own account information. Authorized Allstate Identity Protection staff (customer care and account management teams) have access to employee or family member information based on role and a need-to-know basis. Neither the Board nor OEB have access to information the individual provides to Allstate Identity Protection for the Additional Benefit, or any of the information collected by Allstate Identity Protection in the process of providing either benefit. Allstate Identity Protection provides the OEB with aggregate monthly activation and utilization reports.

5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses):

Employees do not have the opportunity to decline or consent to uses of their information for the automatic Base Benefit. However, employees may decline to register for the Additional Benefit by declining to provide the information required to activate the Additional Benefit. Family members may decline to provide their information, but will still be covered by the Base Benefit, as described above.

6. Procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date:

It is the responsibility of the individual employee or family member to ensure all information provided for the Additional Benefit such as address, date of birth, mailing address, phone number, and/or email address is accurate, complete, and current. If the individual registers for credit monitoring (as part of the Additional benefit), Allstate Identity Protection will validate the Social Security Number if the individual's registration is unsuccessful because of a discrepancy in the information provided. Depending on the individual's choice of communication, the individual will receive an alert from Allstate Identity Protection to correct their personal information over the phone, through Allstate Identity Protection's website, or directly with the credit bureau if information is incorrect.

7. The length of time the data will be retained and how will it be purged:

If an employee is no longer employed by the Board (including through retirement), he or she will have up to 90 days to convert to an individual policy under a separate agreement directly with Allstate Identity Protection. If the former employee takes no action to continue coverage, then with the exception of information needed to support case handling, all other information is deleted from Allstate Identity Protection systems and the former employee must activate their account as a new member to regain coverage.

The case handling information that Allstate Identity Protection retains is limited to ticket detail (open/closed tickets), former employee and/or family member PII (name, address, plan type, email, SSN, activation date/term date), communication alerts, and email/SMS logs. This information is handled in accordance with the record retention schedule laid out in the System of Records entitled BGFRS-29, "FRB—General Benefits Records."

8. The administrative and technological procedures used to secure the information against unauthorized access:

The FedProtect Program adheres to a comprehensive information security policy that applies to all employees, consultants, contractors, and vendors that are deemed necessary to perform services. In addition, Allstate Identity Protection has passed a comprehensive information security review and undergoes continuous monitoring. Data from employees or family members is stored in an encrypted format and transmitted only by secure encrypted connections.

9. Whether a new system of records under the Privacy Act will be created. (If the data are retrieved by name, unique number or other identifier assigned to an individual, then a Privacy Act system of records may be created):

The FedProtect Program is covered by an existing System of Records entitled BGFRS-29, "FRB—General Benefits Records."

Reviewed:

/signed/ ***8/19/2020***
Raymond Romero Date
Senior Agency Official for Privacy

/signed/ ***8/19/2020***
Sharon Mowry Date
Chief Information Officer