



SilverArrow Capital Americas, LLC

PRIVACY POLICY

August 27, 2018

**Protecting your personal information is important to us
We respect your privacy and we are committed to protecting it.
This Privacy Policy explains the way we collect, maintain and handle your personal
information.**

SilverArrow Capital Americas, LLC's Privacy Policy

As a registered investment adviser, SilverArrow Capital Americas, LLC ("SilverArrow") must comply with DC Securities Act and investment adviser rules, which requires registered advisers to adopt policies and procedures to protect the "non-public personal information" of natural person consumers and customers and to disclose to such persons policies and procedures for protecting that information.

Regulation S-P / Privacy Rule

The purpose of these regulatory requirements and privacy policies and procedures is to provide administrative, technical, and physical safeguards which assist employees in maintaining the confidentiality of non-public personal information ("NPI") collected from the consumers and customers of an investment adviser. All NPI, whether relating to an adviser's current or former clients, is subject to these privacy policies and procedures. Any doubts about the confidentiality of client information must be resolved in favor of confidentiality.

For these purposes, NPI includes non-public "personally identifiable financial information" plus any list, description or grouping of customers that is derived from non-public personally identifiable financial information. Such information may include personal financial and account information, information relating to services performed for or transactions entered for clients, advice provided by SilverArrow to clients, and data or analyses derived from such NPI.

Regulation S-P implements the Gramm-Leach-Bliley Act's ("GLB Act") requirements for privacy of consumer nonpublic personal information for registered investment advisers, investment companies, and broker-dealers (each, a "financial institution"). Among other provisions, financial institutions are required to provide an *initial* notice to each customer that sets forth the financial institution's policies and practices for the collection, disclosure, and protection of customers' nonpublic personal information to affiliated and nonaffiliated third parties. Thereafter, as long as the customer relationship continues to exist, the financial institution is required to provide an annual privacy disclosure to its customers describing the financial institution's privacy policies and practices unless it meets the requirements for the annual delivery exception as set forth below.

Significantly, on December 4, 2015, the President signed the *Fixing America's Surface Transportation Act* (the "FAST Act") into law. Among other provisions, the FAST Act includes

an amendment of the consumer privacy provisions within the GLB Act. The amendment, which went into effect immediately, now provides an exception to the *annual* privacy notice distribution requirement if the financial institution meets the following two criteria: (i) the financial institution does not share nonpublic personal information with nonaffiliated third parties (other than as permitted under certain enumerated exceptions); and (ii) the financial institution's policies and practices regarding disclosure of nonpublic personal information have not changed since the last distribution of its policies and practices to its customers.

Regulation S-AM

SEC Regulation S-AM, effective 9/10/2009, with a postponed compliance date from 1/1/2010 to 6/1/2010, requires SEC investment advisers, and other SEC regulated entities, to the extent relevant, to implement limitations on the firm's use of certain consumer information received from an affiliated entity to solicit that consumer for marketing purposes. Regulation S-AM provides for notice and opt-out procedures, among other things. The compliance date was extended to allow registered firms to establish systems to meet the new regulatory requirements.

What personal information do we collect?

In the course of our activities, we collect and hold personal information about you. We will only collect personal information that is necessary to provide our products and services to you, including information needed to comply with legal and regulatory requirements.

We may collect the following types of personal information:

- name;
- email address, mailing or street address, and other contact details;
- date of birth;
- information to verify your identity such as your driver's license number;
- Social Security or EIN;
- bank account details to enable payment of distributions or redemptions;
- margin loan details relevant to your investment in our products; and
- information about other products or services of ours or any related body corporate that you may hold or use.

How do we collect your personal information?

We collect your personal information directly from you unless it is unreasonable or impracticable to do so. When collecting personal information from you, we may collect in ways including:

- from your completion of application forms for our products;
- through your use of our website;
- during communications between you and our representatives; and
- from our conduct of marketing activities which may include requests for more information for example competitions or requesting 'business cards'

We may also collect information about you from additional online and offline sources including commercially available third-party sources, such as credit reporting agencies. We may combine this information with the personal and other information we have collected about you under this Privacy Policy.

We may use the information we collect from you to help us deliver our online services; to administer, evaluate and improve our business (including developing new products and services, improving existing products and services, performing data analytics, and performing accounting, auditing and other internal functions); manage our risks; market our services and products; and to comply with and enforce applicable laws and regulations, relevant industry standards, contractual obligations and our policies. We may also use data that we collect on an aggregate or anonymous basis (such that it does not identify any individual clients) for various business purposes, where permissible under applicable laws and regulations.

What happens if we cannot collect your personal information?

If we do not obtain all the information we need from you, some or all of the following may happen:

- we may not be able to provide you with and subsequently administer some or all our products or services; or
- we may not be able to provide you with information about our products and services.

How is your personal information used?

We will only use your personal information for the purpose of providing you with our investment products and services. In managing your investment, we will use your personal information to:

- assess your application and provide our products and services to you;

- communicate with you in relation to your investment;
- monitor, audit, evaluate and otherwise administer our products and services;
- provide you with access to protected areas of our websites;
- provide continuous service to you and to conduct business processing functions including by providing personal information to our related bodies corporate, contractors, service providers or other third parties; and
- assist with the administrative, marketing (including direct marketing), planning, product or service development, quality control or research purposes of SilverArrow Capital Americas, LLC (“SilverArrow”) and its contractors and service providers.

With whom will we share your personal information?

We share personal information among our affiliates and business units when we believe it will enhance the services we can provide, but only in circumstances where such sharing conforms to law, any applicable confidentiality agreements, and our policies and practices.

We may disclose information we have about you as required or permitted by law. For example, we may share information with regulatory authorities and law enforcement officials when we believe in good faith that such disclosure is necessary to comply with legal requirements. We may share information with third parties where appropriate to protect against fraud or verify or enforce our terms of use, our other rights, or other applicable policies.

From time to time, we enter into agreements with other companies to provide services to us, or to make services and products available to you. Under these agreements, these companies may receive your personal information, but they must safeguard this information, and they may only use it for those purposes we specify.

SilverArrow believes keeping your information secure and private is important, particularly when using third-party websites and applications that may help you invest or manage your finances.

SilverArrow operates as a global organization and to this end, functions generally operate from dedicated centers which also provide shared services around the globe. Personal information (generally other than personal information held in relation to individual investors) may be held within applications on our portfolio management system or client relationship management system which are potentially accessible by our related bodies corporate in any country in which SilverArrow Capital has an office.

We may share your personal information with any person or entity if we have your consent to do so.

Is your personal information secure?

We take our responsibility to protect the privacy and confidentiality of your information, including personal information, very seriously. We maintain physical, electronic, and procedural safeguards that comply with applicable legal standards to secure such information from unauthorized access and use, alteration and destruction. We hold our employees accountable for complying with relevant policies, procedures, rules and regulations concerning the privacy and confidentiality of information.

How can you access your personal information?

You may reach us by mail, phone, fax, or email using the details provided below and request access to your information. Before we give you access to information about you, we will ask you to verify your identity. In normal circumstances we will give you full access to your information; however, at times there may be a legal reason why we must deny access, such as where granting access would interfere with the privacy of others or it would result in a breach of confidentiality. If access is denied we will give you the reasons for any refusal in writing and the mechanisms available to complain about the refusal.

There may be some charge to you to access your information depending on the ease of its retrieval. We will advise you of any cost when you seek the information. We will not charge you for making a request or for making any corrections to your personal information.

Correction of your personal information

We will endeavor to ensure your personal information is kept accurate, complete, up to date, and relevant. Please let us know if any of your details change.

If you believe that the personal information we store about you is incorrect, incomplete, inaccurate, or misleading, you may ask us to amend it. If we do not agree that there are grounds for amendment, we will give you the reasons for any refusal in writing and the mechanisms available to complain about the refusal, and we will add a note to the personal information stating that you disagree with the information.

Robert Schimanko is responsible for reviewing, maintaining, and enforcing these policies and procedures to ensure SilverArrow meets our client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. Mr. Schimanko may recommend to the firm's principal(s) any disciplinary or other action as appropriate. Mr. Schimanko is also responsible for distributing these policies and procedures to employees and conducting appropriate employee training to ensure employee adherence to these policies and procedures.

Dealing with SilverArrow online

We may use “cookies” to help us tailor our website to better suit your needs (e.g., we may use cookies to enable us to save any personal preferences indicated by you) and to provide a more effective route to various components of our website. If you choose to disable cookies, some of our website’s functionality might be impaired. Cookies are small text files that are stored in your computer's memory and hard drive, in your mobile device or tablet when you visit certain web pages. They are used to enable websites to function or to provide information to the owners of a website or other third parties which receive data obtained from that website. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience.

Cookies help us to provide customized services and information. We use cookies to tell us, in general terms, how and when pages in our websites are visited, what our users’ technology preferences are – such as what type of video player they use – and whether our website is functioning properly. Depending on their purpose, some cookies will only operate for the length of a single browsing session, while others have a longer life span to ensure that they fulfil their longer-term purposes (as explained in more detail below). Please note that, however long a cookie’s active life may be, you can delete cookies (and stop any further data collection by them) as further described below.

If you are using a password-protected site, then the website may use cookies or other technology to help us authenticate you, store and recognize your configuration and user attributes, facilitate your navigation of the website and customize its content so that the information made available is likely to be of more interest to you.

In broad terms, we use cookies on our website for the following purposes:

- *Analytical purposes:* Analytical cookies allow us to recognize, measure, and track visitors to the website. This helps us to improve and develop the way the website works, for example, by determining whether site visitors can find information easily, or by identifying the aspects of the site that are of the most interest to them.
- *Usage preferences:* Some of the cookies on the website are activated when visitors to our sites make a choice about their usage of the site. Our website then ‘remembers’ the settings preferences of the user concerned. This allows us to tailor aspects of the site to the individual user.
- *Terms and conditions:* We use cookies on the website to record when a site visitor has seen a policy, such as this one, or provided consent, such as consent

to the terms and conditions on our website. This helps to improve the user's experience of the site – for example, it avoids a user from repeatedly being asked to consent to the same terms.

- *Session management*: The software that runs the website uses cookies for technical purposes needed by the internal workings of our servers. For instance, we use cookies to distribute requests among multiple servers, authenticate users and determine what features of the site they can access, verify the origin of requests, keep track of information about a user's session and determine which options or pages to display in order for the site to function.
- *Functional purposes*: Functional purpose cookies store information that is needed by our applications to process and operate. For example, where transactions or requests within an application involve multiple workflow stages, cookies are used to store the information from each stage temporarily, in order to facilitate completion of the overall transaction or request.
- *Advertising*: Advertising cookies allow us (or third parties) to monitor the behavior of users of our website. This information is used to ensure that products and services highlighted to those individuals are targeted in a focused and relevant manner – e.g. through advertisements on our website or through advertisements on third party websites which are based on your experience with our website; or to monitor the effectiveness of those digital marketing campaigns. We also monitor whether the adverts displayed on our website are of interest to users and retain this information to ensure that adverts seen by users of our website over a period of time are appropriate.

You can configure your browser to accept all cookies, reject all cookies, notify you when a cookie is set, or delete cookies that have already been set. Each browser is different, so check the "Help" menu of your browser to learn how to change your cookie preferences. You are always free to decline our cookies if your browser permits, although in that case you may not be able to use certain features on our website.

We may include content on the website designed for display using Adobe Flash Player, such as animations, videos, and tools. Local flash storage (often referred to as "Flash cookies") can be used to help improve your experience as a user. Flash storage is retained on your device in the same way as standard cookies, but is managed directly by your Flash software. If you wish to disable or delete information stored locally in Flash, please see the documentation for your Flash software, located at www.adobe.com. Please note that, if you disable Flash cookies, some site functionality may not work.

When you visit our website, you may receive cookies set by third parties. The kind of cookies and the consequent data processing carried out by such third parties are regulated by the third party's privacy policy. We do not control the setting of these third party cookies. You may wish to check any such third party's website for more information about their use of cookies and how to manage them.

We notify you when our privacy policies and practices change.

SilverArrow is not required to deliver an annual privacy notice provided it: (1) only shares NPI with nonaffiliated third- parties in a manner that does not require an opt-out right be provided to customers (e.g., if the institution discloses NPI to a service provider or for fraud detection and prevention purposes); and (2) has not changed its policies and practices with respect to disclosing NPI since it last provided a privacy notice to its customers.

If, at any time, SilverArrow adopts material changes to its privacy policies, the firm shall provide each such client with a revised notice reflecting the new privacy policies. The Compliance Officer is responsible for ensuring that required notices are distributed to the SilverArrow's consumers and customers.

Opt Out Rights and Procedures

You may contact us at (202) 331-7900, or send an email to our Compliance Officer, Robert Schimanko, schimanko@silverarrowcapital.com, to discuss this information in more detail or to request to "Opt-Out" our release of your non-public personal information to optional third parties. Please be aware that the "Opt Out" provisions do not apply for any disclosures of NPI SilverArrow makes to service providers or joint marketers, but SilverArrow will disclose the nature of any information to be shared with a service provider or joint marketer, and SilverArrow will enter into contractual arrangements to require the third party to maintain confidentiality of your information.

The Opt-Out rights also do not apply to disclosure of confidential information in the following circumstances: 1) when you have consented to, and have not revoked, the disclosure of NPI; 2) for resolving consumer or customer disputes or inquiries; 3) to persons holding a legal or beneficial interest relating to you; 4) to persons acting in a fiduciary or representative capacity on your behalf; 5) to provide information to agencies assessing SilverArrow's compliance with industry standards, and to the SilverArrow's attorneys, accountants, and auditors in connection with a proposed or actual sale or merger of SilverArrow; 6) to respond to a regulator's examination of SilverArrow; or 7) to comply with a civil, criminal, or regulatory investigation by federal, state, or local authorities. Additionally, we will not revise our Policy to permit the sharing of non-public personal information other than described unless we first notify you and provide you with the opportunity to prevent the sharing of information.

What is the process for complaining about a breach of privacy?

If you believe your privacy has been breached, please contact our Privacy Officer using the contact information below and provide details of the incident so that we can investigate it.

We request that complaints about breaches of privacy be made in writing, so we can be sure about the details of the complaint. We will attempt to confirm as appropriate and necessary with you, your understanding of the conduct relevant to the complaint and what you expect as an outcome. We will inform you of whether we will conduct an investigation, the name, title, and

contact details of the investigating officer and the estimated completion date for the investigation process.

After we have completed our enquiries, we will contact you, usually in writing, to advise the outcome and invite a response to our conclusions about the complaint. If we receive a response from you, we will assess it and advise if we have changed our view.

Safeguarding and Disposal of Client Information

SilverArrow restricts access to NPI to those employees who need to know such information to provide services to our clients.

Any employee who is authorized to have access to NPI is required to keep such information secure. All electronic or computer files containing such information shall be secured and firewall protected from access by unauthorized persons. Any conversations involving NPI, if appropriate at all, must be conducted by employees in private, and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Safeguarding standards encompass all aspects of SilverArrow that affect security. This includes not just computer security standards but also such areas as physical security and personnel procedures. Examples of important safeguarding standards SilverArrow may adopt include:

- access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means (*e.g.*, requiring employee use of user ID numbers and passwords, etc.);
- access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals (*e.g.*, intruder detection devices, use of fire and burglar resistant storage devices);
- encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- procedures designed to ensure that customer information system modifications are consistent with the firm's information security program (*e.g.*, independent approval and periodic audits of system modifications);
- dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information (*e.g.*, require data entry to be reviewed for accuracy by personnel not involved in its preparation; adjustments and correction of master records should be reviewed and approved by personnel other than those approving routine transactions, etc.);

- monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems (*e.g.*, data should be auditable for detection of loss and accidental and intentional manipulation);
- response programs that specify actions to be taken when the firm suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies;
- measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures (*e.g.*, use of fire resistant storage facilities and vaults; backup and store off site key data to ensure proper recovery); and
- information systems security should incorporate system audits and monitoring, security of physical facilities and personnel, the use of commercial or in-house services (such as networking services); and
- contingency planning.

Any employee who is authorized to possess "consumer report information" for a business purpose is required to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. There are several components to establishing 'reasonable' measures that are appropriate for the firm:

- assessing the sensitivity of the consumer report information we collect;
- the nature of our advisory services and the size of our operation;
- evaluating the costs and benefits of different disposal methods; and
- researching relevant technological changes and capabilities.

Some methods of disposal to ensure the information cannot practicably be read or reconstructed that SilverArrow may adopt include:

- procedures requiring the shredding of papers containing consumer report information;
- procedures to ensure the destruction or erasure of electronic media; and
- after conducting due diligence, contracting with a service provider engaged in the business of record destruction, to provide such services in a manner consistent with the disposal rule.

Whom can you reach at SilverArrow?

If you have any queries or concerns about the privacy of your information, please contact our Privacy Officer via the following:

Robert Schimanko

Phone: 202.331.7900

Facsimile: 202.664.8383

Email: schimanko@silverarrowcapital.com

Mail: 1320 19th Street, NW Suite 601 Washington, D.C. 20036

Please address all written requests:

Attention: SilverArrow Capital Americas, LLC

Privacy Officer