

To California Residents: We take your privacy very seriously. Please read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use, and share your personal information. It also explains your rights under California law in relation to your personal information and how to contact us or supervisory authorities in the event you have a complaint. This notice is intended to comply with the California Consumer Privacy Act of 2018 (**CCPA**) and the California Privacy Rights Act of 2021 (**CPRA**), as well as any other applicable data privacy laws, and any terms defined in the CCPA and CPRA have the same meaning when used in this notice.

1. Key Terms. It would be helpful to start by explaining some key terms used in this policy:

We, us, our	Mid Atlantic Trust Company; Mid Atlantic Capital Group, Inc.; American Trust Company; AT Retirement Services, LLC; AmericanTCS Technology, LLC.; Collectively, all of our companies are part of the AmericanTCS group of companies and are referred as “AmericanTCS” throughout this policy.
Consumer, you, your	Any natural person who is a resident in the state of California for other than a temporary purpose or domiciled in the state of California and outside of the state for a temporary or transitory purpose
Employee, applicant	Any natural person who is a resident in the state of California for other than a temporary purpose or domiciled in the state of California and outside of the state for a temporary or transitory purpose who is a current, past, or prospective job applicant, employee, worker, member, or temporary worker or contractor of AmericanTCS.

Our data protection officer	Bob Drelick, CIO/CISO AmericanTCS
Personal information	Information that identifies, relates to, describes or is capable of being associated with or linked to a particular consumer or household, excluding deidentified data and aggregate information.

2. Personal Information We Collect About You. We may collect and use the following personal information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, employee or applicant:

Categories of Personal Information	Specific Types of Personal Information Collected
Identifiers (e.g., real name or alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or similar)	Name, mailing address, username, email address, social security number, driver's license number, passport number
Information that identifies, relates to, describes, or is capable of being associated with, a particular consumer (e.g., name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number,	Name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, employment, bank account number, other financial information

insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information)	
Sensitive personal information of Employees and Applicants	Name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, employment, bank account number, other financial information; precise geolocation; an individual's racial or ethnic origin, religious or philosophical beliefs, or union membership; the contents of an individual's mail, email, and text messages unless We are the intended recipient of the communication; genetic data; biometric information used to uniquely identify the individual; personal information collected and analyzed regarding an individual's health; and personal information collected and analyzed regarding an individual's sex life or sexual orientation
Protected categories of information collected regarding Employees and Applicants	Age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related

	medical conditions), sexual orientation, veteran or military status, genetic information (including familial), AIDS/HIV status, medical condition, political activities or affiliations, and status as a victim of domestic violence, assault, or stalking
Characteristics of protected classifications under California or federal law.	To the extent stated on government-issued identification documents (e.g., driver's license, passport): race, ethnicity, gender, national origin, age
Commercial information (e.g., records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies)	Consumers: We do not collect; Employees and Applicants: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
Biometric information	Fingerprints (certain employees only)
Internet or other electronic network activity information (e.g., browsing history, search history, information regarding a consumer's interaction with an internet website application, or advertisement)	Consumers: We do not collect; Employees and Applicants: browsing history, search history, information regarding a consumer's interaction with an internet website application, or advertisement
Geolocation data	Consumers: We do not collect;

	Employees and Applicants: physical location
Audio, electronic, visual, thermal, olfactory, or similar information	Consumers: We do not collect; Employees and Applicants: audio, electronic, visual, thermal, olfactory, or similar information
Professional or employment-related information	Consumers: Employment-related information as it concerns personal investment accounts or retirement accounts; Employees and Applicants: job preference and work availability, qualifications, employment history and experience, compensation, military service, reference and background check information, including relevant criminal history and credit history, pre-employment test results, post-offer medical and medical examination information and results, including drug test results, immigration and work eligibility, and information provided by you during the interview and hiring process
Non-public education information that is personally identifiable information, as defined in the Family Educational Rights and Privacy Act (FERPA)	Consumers: We do not collect; Employees and Applicants: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student

	financial information, or student disciplinary records.
Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes	Consumers: We do not collect; Employees and Applicants: profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

For Consumers, this personal information is required to provide products and/or services to you;

For Employees and Applicants, this personal information is required for candidate selection, hiring and employment purposes.

If you do not provide personal information we request, it may delay or prevent us from providing products and/or services to you.

3. How Your Personal Information is Collected. We collect most of this personal information from your employer or directly from you in person, by telephone, by text or email and/or via our secure website. For Employees and Applicants: We collect most information directly from you, for example from applications, questions you might answer as an Employee, internal software applications and systems, schedules and forms. However, we may also collect information:

- From publicly accessible sources (e.g., property records);
- Directly from a third party (e.g., sanctions screening providers, credit reporting agencies, or customer due diligence providers);

- From a third party with your consent (e.g., your bank);
- From cookies on our website; and
- Via our IT systems, including:
 - Door entry systems and reception logs; and/or
 - Automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, email and instant messaging system.

You have a right to correct your personal information in our records. However, in some cases we may require authorization from the source of this personal information prior to correcting it in our records. For example, if you are a participant in an employer retirement plan, and request that we correct your mailing address, your employer may need to authorize that correction, as the address in our records must match the address in your employer's records. If you make a request for correction of your personal information we will explain any such additional considerations specific to your request.

4. How and Why We Use Your Personal Information.

Consumers: Under data protection law, we can only use your personal information if we have a proper reason for doing so, such as:

- To comply with our legal and regulatory obligations;
- For the performance of our contract with you or to take steps at your request before entering into a contract;
- For our legitimate interests or those of a third party; or
- Where you have given consent.

Employees and Applicants:

- To comply with our legal and regulatory obligations;
- To fulfil the usual human resources function obligations, such as, administration, payroll and general management;
- To have a global and consistent reporting system and processing of compensation and benefits as well as reporting of diversity reports or for long term incentive plans, where entitled; or to maintain records and ensure the accuracy of each Employee's details on compensation and benefits;
- To allow human resources staff and line management to carry out talent management, succession planning and succession management, by capturing, analyzing and reporting the data relating to Employees;
- To ensure proper compensation and benefits via external and internal benchmarking;
- To know what career aspirations, development plans and progression each Employee has and to achieve global visibility of such information;
- To assess regulatory compliance and to carry out investigations into workplace conduct including, where permitted by local law, the monitoring of correspondence stored and created on Employee's work-issued devices;
- To gain operational visibility, monitor workplace efficiency and quality;
- To ensure cost-effectiveness and appropriate company administration;
- To analyze and prepare the company, function or department for any structural changes or shifts;
- To defend in any litigation to third party claims or to bring claims to protect the rights of the company or protect against damage, injury, theft, legal liability, fraud, abuse or other misconduct;

- To conduct internal disciplinary, grievance and termination processes or to review and assess compliance with company policies;
- To maintain and monitor usage of internal networks and the information technology systems in line with our guidelines and policies;
- To conduct legal proceedings (including prospective legal proceedings), and obtain legal advice;
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations; and
- As described to you when collecting your personal information or as set forth in the CCPA and CPRA.

A legitimate interest is when we have a business or commercial reason to use your information, so long as this is not overridden by your own rights and interests.

The table below explains how we use your personal information and our reasons for doing so:

We use your personal information for:	Our reasons for use:
To provide you with services related to your personal investment account(s) or your retirement plan account(s)	For the performance of our contract with or concerning you
To prevent and detect fraud against you or the entity or entities responsible for your personal investment account(s) or your retirement account(s)	For our legitimate interests or those of a third party, i.e., to minimize fraud that could be damaging for us and for you
Conducting checks to identify our customers and verify their identity; Screening for financial and other	To comply with our legal and regulatory obligations

sanctions or embargoes; Other processing necessary to comply with professional, legal and regulatory obligations that apply to our business, e.g. under fraud prevention laws or rules issued by our professional regulators	
Gathering and providing information required by or relating to audits, inquiries or investigations by regulatory bodies	To comply with our legal and regulatory obligations
Ensuring business policies are adhered to, e.g. policies covering security and internet use	For our legitimate interests or those of a third party, i.e., to make sure we are following our own internal procedures so we can deliver the best service to you
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests or those of a third party, i.e., to be as efficient as we can so we can deliver the best service for you at the best price
Ensuring the confidentiality of commercially sensitive information	For our legitimate interests or those of a third party, i.e., to protect trade secrets and other commercially valuable information; To comply with our legal and regulatory obligations
Statistical analysis to help us manage our business, e.g., in relation to our financial performance, customer base, product range or other efficiency measures	For our legitimate interests or those of a third party, i.e., to be as efficient as we can so we can deliver the best service for you at the best price

Preventing unauthorized access and modifications to systems	For our legitimate interests or those of a third party, i.e., to prevent and detect criminal activity that could be damaging for us and for you; To comply with our legal and regulatory obligations
Updating and enhancing customer records	For the performance of our contract with or concerning you; To comply with our legal and regulatory obligations; For our legitimate interests or those of a third party, e.g., ensuring we can promptly and efficiently provide services concerning your account(s)
Statutory returns	To comply with our legal and regulatory obligations
Ensuring safe working practices, staff administration and assessments	To comply with our legal and regulatory obligations; For our legitimate interests or those of a third party, e.g., to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
Marketing our services and those of selected third parties to: existing and former customers; third parties who currently benefit from or receive, or who have previously benefitted from or received, our services.	For our legitimate interests or those of a third party, i.e. to promote our business to existing and former customers

Credit reference checks via external credit reference agencies	For our legitimate interests or those of a third party, e.g., as part of or in connection with employee background checks
External audits and quality checks, e.g., for the audit of our accounts	For our legitimate interests or a those of a third party, i.e., to maintain our accreditations so we can demonstrate we operate at the highest standards; To comply with our legal and regulatory obligations

5. Promotional Communications. For **Consumers**, we may use your personal information to send you updates (by regular mail or email) about our products and/or services, including promotions or new products and/or services.

We have a legitimate interest in processing your personal information for promotional purposes (see “How and Why We Use Your Personal Information,” above). This means we do not usually need your consent to send you promotional communications. However, where consent is needed, we will ask for this consent separately and clearly.

We will always treat your personal information with the utmost respect and never, for marketing purposes, sell that information to or share it with other organizations outside of AmericanTCS.

You have the right to opt out of receiving promotional communications at any time by:

- Using the “unsubscribe” link in emails; or
- Submitting a request according to “How to Contact Us,” below.

We may ask you to confirm or update your marketing preferences if you instruct us to provide further products and/or services in the future, or if there are changes in the law, regulation, or the structure of our business.

6. Who Has Access to Your Personal Information: We occasionally share Consumers', Employees' and Applicants' personal information with:

- Our affiliates, including companies within AmericanTCS (as defined above);
- Service providers, with whom we contract to supply you with our products and services, such as payment, recordkeeping and other administrative service providers;
- Other contractors with whom we contract to help us run our business, such as website hosts;
- Our insurers and brokers; and
- Our bank(s).

We only allow our service providers and contractors to handle your personal information if we are assured that they take appropriate measures to protect your personal information. We also impose contractual obligations on service providers and contractors in order to ensure that they protect your personal information and only use your personal information to provide services to us and to you. We may also share personal information with external auditors, as appropriate and necessary to accomplish an audit of our accounts.

We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.

We may also need to share some personal information with other parties, such as potential buyers of some or all of our business or during a re-structuring. We will typically anonymize information, but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

Consumers: We will not share your personal information, including such information we may hold for consumers under 16 years of age, except as necessary to conduct our business operations and provide you with the products and services related thereto.

Employees and Applicants: We will not share your personal information, except as necessary for employment and related services and to conduct our business.

Sensitive personal information is defined as: 1) personal information that reveals a consumer's: various specific identity numbers; various accounts' security access data; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, or union membership; contents of mail, email, and text messages; genetic data; and 2) the processing of biometric information for the purpose of uniquely identifying a consumer; and personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.

Consumers: AmericanTCS does not use or disclose sensitive personal information other than for providing services to you as described above.

Employees and Applicants: AmericanTCS does not use or disclose sensitive personal information except as necessary for employment and related services and to conduct our business.

7. Personal Information Sold or Disclosed for a Business Purpose. We do not sell your personal information, including any such information we may hold for consumers under 16 years of age. In the preceding 12 months, we have disclosed for a business purpose to one or more third parties the following categories of personal information that identify, relate to, describe, is capable of being associated with or which could reasonably be linked, directly or indirectly, with a particular consumer or household:

- Identifiers (e.g., a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name or username, social security number, driver's license number, passport number, or other similar identifiers);

- Other information that identifies, relates to, describes or is capable of being associated with a particular Consumer, Employee or Applicant, including, but not limited to their: signature, social security number, physical characteristics or description, telephone number, passport number, state identification card number, employment, bank account number or other financial information;
- Characteristics of protected classifications under California or federal law;
- Commercial information;
- Biometric information (AmericanTCS employees only);
- Internet or other electronic network activity information regarding a consumer's interaction with an internet website, application, or advertisement;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (FERPA); and
- Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Sensitive personal information of Employees and Applicants (for example, sharing data with Benefits Providers)
- Protected categories of information collected regarding Employees and Applicants

8. Where Your Personal Information is Held. Information may be held at our offices and those of our affiliates and associated persons or representatives, as well as with third party agencies, service providers, representatives and agents as described above (see above: "Who We Provide with Your Personal Information," above).

9. How Long Your Personal Information Will Be Kept.

Consumers: We will keep your personal information while you have an account with us or while we are providing products and/or services to you. Thereafter, we will keep your personal information for as long as is necessary:

- to respond to any questions, complaints or claims made by you or on your behalf;
- to show that we treated you fairly; or
- to keep records, and for the duration of any record retention period(s), required by law.

Employees and Applicants: We will keep your personal information during the application process for applicants, and for the duration of your employment for employees. Thereafter, we will keep your personal information as long as is necessary:

- to respond to any questions, complaints or claims made by you or on your behalf;
- to show that we treated you fairly; or
- to keep records, and for the duration of any record retention period(s), required by law.
- For **Applicants** not hired: your personal information will be kept for one year after application;
- For **Employees**: your personal information will be kept for up to seven years after your employment ends, though certain agreements and contracts may be kept permanently.

We will not retain your personal information for longer than necessary for the purposes set out in this policy. Different retention periods apply to different types of personal information, but generally we retain records (including those containing personal information) for up to seven years, in accordance with applicable requirements

under statutes and regulations promulgated by federal regulators and their authorized delegates (e.g., Securities and Exchange Commission, Internal Revenue Service, Department of Labor).

When it is no longer necessary to retain your personal information, we will delete or anonymize it.

10. Keeping Your Personal Information Secure. We have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorized way. We limit access to your personal information to those who have a genuine business need to access it. Those processing your information will do so only in an authorized manner and are subject to a duty of confidentiality. We continually test our systems ensuring we proactively monitor for new threats and we follow industry standards for information security. We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator in the event of a suspected data security breach and where we are legally required to do so.

11. How to Exercise Your Rights. If you would like to exercise any of your rights as described in this Privacy Policy, including your right to know your personal information in our records, please see below.

Consumers may:

- Complete a data subject request form available on our website at <https://www.americanctcs.com/>, CCPA Request button;
- Call us, toll-free, at 833-855-5838

Employees and Applicants may:

- Call us, toll-free, at 800-693-7800

We do not sell your personal information. We do not share your personal information, including sensitive personal information, other than with service providers and contractors employed by us to provide services to you as described above.

Please note that you may only make two CCPA-related data access or data portability disclosure requests within a 12-month period.

If you choose to contact us using any of the methods above, you will need to provide us with:

- Enough information to identify you (e.g., your full name, address AND account name/number);
- Proof of your identity and address (e.g., a copy of your driver's license, state identification card or passport AND a recent utility or credit card bill); and
- A description of the right you wish to exercise and the information to which your request relates.

We are not obligated to make a data access or data portability disclosure if we cannot verify that the person making the request is either the person about whom we collected information or someone authorized to act on such person's behalf.

Any personal information we collect from you to verify your identity in connection with your request will be used solely for the purposes of verification.

12.Changes to This Privacy Notice. This privacy notice was published on January 1, 2020, and last updated on July 31, 2026.

We may change this privacy notice from time to time. When we do, we will inform you via our website or, only where appropriate, other means of contact such as email.

13.How to Contact Us. Please contact us by mail, email or telephone if you have any questions about this privacy policy or the information we hold about you. You may also submit a request directly through our website by clicking the “CCPA Requests” link.

Our contact details are shown below:

Our Contact Details	Our Data Protection Officer’s Contact Details
Bob Drelick, Chief Information Officer & Chief Information Security Officer	1251 Waterfront Place, Suite 510 Pittsburgh, PA 15222
(833) 855-5838	(833) 855-5838
Employees and Applicants may call: 800-693-7800	

14.Do You Need Extra Help? If you would like this notice in another format (for example: audio, large print, braille) please contact us (see “How to Contact Us,” above).