

Effective Date: 07-01-2024

PRIVACY NOTICE

PURSUANT TO THE FLORIDA DATA PRIVACY AND SECURITY ACT

This Florida privacy notice (“Notice”) pursuant to the Florida Data Privacy and Security Act, Florida Code § 501.701 et seq., (“FDPSA”), supplements the information contained in the Privacy Policy of Rausch Sturm LLP (“Rausch Sturm,” “we,” “us,” or “our”), and applies solely to visitors, users, and others who reside in the State of Florida (“consumers” or “you”). Rausch Sturm is a debt collector. This Notice applies to both our online and offline practices. We adopt this Notice to comply with the FDPSA. Any terms defined in the FDPSA have the same meaning when used in this Notice. For questions concerning this Notice or to obtain a copy of this Notice in an alternative format or in Spanish, please call us at 855-517-6279.

A. Consumer Rights

The FDPSA provides consumers with specific rights regarding their personal data. This section describes your rights.

1. **Right of Confirmation:**

You have the right to confirm whether we are processing your personal data and to access your personal data.

2. **Right to Correct:**

You have the right to correct inaccuracies in your personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data.

3. **Right to Deletion:**

You have the right to delete any or all personal data provided by or obtained about you.

4. **Right to Data Portability:**

You have the right to obtain a copy of your personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format.

5. **Right to opt out:**

You have the right to opt out of the processing of personal data concerning you for purposes of:

- i. Targeted advertising;
- ii. The sale of personal data;
- iii. Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning you.

We will not sell your personal data. Nor will we process your personal data for the purpose of targeted advertising. We will not engage in profiling in the processing of personal data. If in the future, we anticipate selling your personal data or processing your personal data for purposes of targeted advertising or profiling, we will provide you with the opt-out rights pursuant to the FDPSA.

6. **Right to opt out:**

You have the right to opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data. We will not collect or process your sensitive data without first presenting you with clear notice and an opportunity to opt out of the processing.

7. Right to opt out

You have the right to opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

We do not collect personal data through the operation of a voice recognition or facial recognition feature.

B. Our Duties

1. The FDPSA requires that we provide you with the following information.

i. Categories of personal data processed by us:

- Personal identifying information, like name, address and account number, as well as other identifying information, which we obtain from the consumer's creditor, credit reports and other skip trace tools, and the consumer;
- Characteristics such as age, gender, etc., which we obtain from the consumer's creditor and consumer's credit report;
- Retail information, which we obtain from the consumer's creditor and the consumer's credit report;
- Commercial information, including records of personal property;
- Internet activity regarding online payments and account updates, which we collect if the consumer visits our website or payment portal;
- Geolocation data, which we obtain from process servers;
- Recordings, which are made when the consumer has a telephone conversation with us;
- Professional and employment related information, which we obtain from the consumer's creditor, credit reporting agencies, the consumer, and other skip trace sources; and
- Educational information, which we obtain from the consumer's creditor, credit reporting agencies, the consumer, and other skip trace sources.

ii. Purpose of processing personal data:

- Helping to ensure security and integrity to the extent the use of personal data is reasonably necessary and proportionate for these purposes;
- Debugging to identify and repair errors that impair existing intended functionality;
- Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of consumer's current interaction with the business, provided that the consumer's personal data is not disclosed to

another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with us.

- Performing services on our behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
 - Undertaking internal research for technological development and demonstration.
 - Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufacture for, or controlled by the business.
 - Other business or business operational purposes as follows:
 - Debt collection.
 - To fulfill or meet the reason for which the information is provided. For example, if you provide us with personal data in order for us to process a payment, we will use that information to process said payment.
 - To provide you with information or services that you request from us.
 - To provide you with email or text alerts and other notices concerning our services.
 - To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for collections.
 - To carry out our obligations and enforce our rights arising from any contracts entered into between you and our clients, including for collections.
 - To improve our website and present its contents to you.
 - For testing, research, analysis and service development.
 - As necessary or appropriate to protect the rights, property or safety of us, our clients or others.
 - To respond to law enforcement requests and as required by applicable law, court order, governmental regulations, or comply with a court order or subpoena to provide information.
 - As described to you when collecting your personal data or as otherwise set forth in the Florida collection laws.
- iii. How you may exercise your rights, including the process by which you may appeal our decision with regard to your request:

- When you exercise your rights, we will use commercially reasonable methods for authenticating the identity of the person submitting a request to exercise rights.
 - When you exercise your rights, we will respond without undue delay, which may not be later than 45 days after the date of the receipt of the request. We may extend the response period once by an additional 15 days when reasonably necessary, taking into account the complexity and number of the consumer's request, so long as we inform you of the extension within the initial 45 day response period, together with the reason for the extension.
 - If we cannot take action regarding your request, we must inform you without undue delay, which may not be later than 45 days after the date of receipt of the request, of the justification for the inability to take action on the request and provide instructions on how to appeal the decision.
 - We have established an appeal process by which you may appeal any refusal of ours to take action on a request. We will inform you in writing of any action taken or not taken in response to an appeal within 60 days after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.
- iv. Categories of personal data that we share with third parties:
- Personal identifying information
 - Characteristic information
 - Retail information
 - Professional or employment related information
- v. Description of the methods by which consumers can submit requests to exercise their consumer rights:
- Submission: To exercise the access, deletion, correction or appeal rights described above, please submit a verifiable consumer request to us by either:
 - Calling us at 855-517-6279
 - Submitting the submission form located at:
www.rauschsturm.com/request-FL
2. We will not sell your personal data, including sensitive data. If in the future, we anticipate selling your personal data, including sensitive data, we will provide you with the opt-out rights pursuant to the FDPSA.
3. We will not sell your personal data, including biometric data. If in the future, we anticipate selling your personal data, including your biometric data, we will provide you with the opt-out rights pursuant to the FDPSA.

4. We will not sell your personal data to third parties or process personal data for targeted advertising. If in the future, we anticipate selling your personal data to third parties or processing your personal data for purposes of targeted advertising, we will provide you with the opt-out rights pursuant to the FDPSA.
5. We will not collect additional categories of personal information or use personal information collected for additional purposes without providing you with notices as required by the FDPSA.

C. Limitations

The above rights and duties may be limited if any of the following apply:

1. We are both a controller and a processor as those terms are defined by the FDPSA. A processor that is a controller shall comply with the FDPSA with regard to any personal data that it collects or maintains outside of its role as a processor. Most of the personal data that we collect or maintain is done in context of our role as a processor. If we deny your verified request pursuant to this notice because all of the information collected or maintained about you has been pursuant to our role as a processor, we will provide you with the contact information of the business on whose behalf we collect or maintain the information.
2. The FDPSA does not apply to:
 - i. Protected health information under the Health Insurance Portability and Accountability Act of 1966, 42 USC ss. 1320d et seq.
 - ii. Health records.
 - iii. Patient identifying information for purposes of USC s. 290dd-2.
 - iv. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section which is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1966, 42 USC ss 1320d et seq or by a program or a qualified service organization.
 - v. The collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, or by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15, USC ss 1681 et seq.
 - vi. Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC ss 2721 et seq.
 - vii. Data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller,

processor, or third party, to the extent that the data is collected and used withing the context of that role.

- viii. Data processed or maintained as the emergency contact information of an individual under this part which is used for emergency contact purposes.
 - ix. Data that is processed or maintained and that is necessary to retain to administer benefits for another individual which relates to individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party and which is used for the purposes of administering those benefits.
 - x. Personal data collected and transmitted which is necessary for the sole purpose of sharing such personal data with a financial service provider solely to facilitate short-term, transactional payment processing for the purchase of products or services.
 - xi. Personal data shared between a manufacturer of a tangible product and authorized third-party distributors or vendors of the product, as long as such personal data is used solely for advertising, marketing, or servicing other product that is acquired directly through such manufacturer and such authorized third-party distributors or vendors.
 - xii. the processing of personal data by a person in the course of a purely personal or household activity or solely for measuring or reporting advertising performance, reach, or frequency.
3. Compliance would restrict our ability to:
- i. comply with a federal, state, or local law, rule, or regulation;
 - ii. comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental entity;
 - iii. investigate, establish, exercise, prepare for, or defend a legal claim;
 - iv. provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;
 - v. take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;
 - vi. prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;
 - vii. Preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security;
 - viii. assist another controller, processor or third party in complying with the requirements of the with an obligation of FDPSA;

- ix. disclosure personal data disclosed when a consumer uses or directs the controller intentionally interact the third party. And intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumers intent to interact with the third party.
 - x. transfer personal data to a third party as an asset that is a part of a merger, an acquisition, a bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that the information is used or shared in the manner consistent with this part. If a third party materially alters how it uses or shares the personal data of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it must provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with this part.
4. Compliance would adversely affects the right rights or freedoms of any person, including the right of free speech;
5. Compliance would prevent us from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.
6. Compliance would prevent us or a consumer to disclose a trade secret;
7. Compliance would restrict our ability to collect, use, or retain data to do any of the following:
 - i. conduct internal research to develop, improve, or repair products, services, or technology;
 - ii. effect a product recall;
 - iii. identify and repair technical errors that impair existing or intended functionality;
 - iv. perform internal operations that are:
 - reasonably aligned with the expectations of the consumer
 - reasonably anticipated based on the consumers existing relationship with the controller.
 - otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.
8. Compliance would violate an evidentiary privilege under the laws of this state.
9. We are unable to authenticate a request made under the FDPSA using commercially reasonable efforts.
10. Compliance would require us to do any of the following:
 - i. reidentify deidentified data or pseudonymous data;

- ii. maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or
 - iii. comply with an authenticated consumer request to exercise a right if: (i) (A) the controller is not reasonably capable of associating the request with the personal data; or (B) it would be unreasonably burdensome for the controller to associate the request with the personal data; (ii) the controller does not: (A) use the personal data to recognize or respond to the consumer who is the subject of the personal data; or (B) associate the personal data with other personal data about the consumer; and (iii) the controller does not sell or otherwise disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.
11. The information is pseudonymous data and the controller demonstrates that any information necessary to identify a consumer is kept: (a) separately; and (b) subject to appropriate technical and organizational measures to ensure the personal data are not attributed to an identified individual or an identifiable individual.
12. The information is pseudonymous data or deidentified data and the controller takes reasonable steps to ensure that it: (a) complies with any contractual obligations to which the pseudonymous data or deidentified data are subject; and (b) promptly addresses any breach of a contractual obligation.

D. Changes To Our Privacy Notice

This Notice was last updated on 01-01-2025. We reserve the right to amend this Notice at our discretion and at any time. When we make changes to this Notice, we will notify you by updating the “last updated” date on this notice.

This communication is from a debt collector.