ThreatMetrix Processing Notice

Last updated: 11th May 2022

About This Processing Notice

ThreatMetrix, Inc. (“ThreatMetrix”), a LexisNexis Risk Solutions Group (“RSG”) company, helps organizations to protect against online fraud and criminal activity and to authenticate users of online services. This processing notice explains how ThreatMetrix processes personal information as part of our services for our organizational customers (collectively, “Customers” and each, a “Customer”). Use of ThreatMetrix services is governed by the applicable agreements and the LexisNexis Risk Solutions Group Privacy Policy.

Information Processed

Our Customers choose which personal information of their clients and prospective clients (collectively, “Clients” and each, a “Client”) ThreatMetrix is authorized to receive, such as names, mobile phone numbers, email addresses, mailing addresses, location information, credit card and other payment information, behavioral biometrics and device identifiers. This data is automatically tokenized upon receipt. Tokenization is a pseudonymization measure that turns an identifier, such as an account number, into a random string of characters called a token, for example ‘dh57rh395jf8j02oj94kt784h’. Tokens are used to represent the original identifier but cannot be used to re-identify the data. The tokens are then matched across different Customers’ submissions throughout the LexisNexis Digital Identity Network and combined into a unique digital identifier: the “LexID Digital”.

We also process personal information linked to the LexID Digital in a pseudonymous form, including, but not limited to: (i) the number of email addresses and phone numbers associated with a Client’s internet-connected devices; (ii) activities and attributes associated with a Client’s email addresses, shipping addresses, phone numbers, IP addresses; (iii) device fingerprinting information and activities associated with other online IDs, passwords and drivers’ license numbers, which have been hashed by the Customer prior to being provided to us; (iv) Client account details, log-in activity and history; and (v) Client transaction history associated with hashed payment card identifiers, tracked over time, together with associated risk scores created or used by us through the use of the services (collectively, “attribute information”).

We may also process similar categories of personal information received from other RSG companies and our service providers to improve the predictive insights of data.

Purposes and Legal Basis for Processing

We process personal information for the legitimate interests of us and our Customers for:

- identity verification;
- detection, investigation, assessment, monitoring and prevention of fraud and other crime;
- mitigation of financial and business risk; and/or compliance with anti-money laundering (AML), counter-terrorism financing (CTF), anti-bribery and corruption (ABC) and other regulatory requirements.

We may also use personal information for the enhancement of our services, including refining of analytics capabilities and development of new attributes, models and scores, analyzing established and anomalous pattern detection and graph analysis.
Information Recipients

We share attribute information:

- with our Customers, our processors, our sub-processors and other RSG companies;
- where we have a good faith belief that such disclosure is necessary to meet any applicable law, regulation, legal process or other legal obligation; detect, investigate and help prevent security, fraud or technical issues; and/or protect the rights, property or safety of ThreatMetrix, the RSG companies, our users, our employees or others; and
- as part of a corporate transaction, such as a transfer of assets or an acquisition by or merger with another company.

Data Retention

We retain personal information for only as long as necessary to provide the services and fulfill the transactions requested by our Customers, or for other essential purposes such as complying with our legal obligations, maintaining business and financial records, resolving disputes, maintaining security, detecting and preventing fraud and abuse, and enforcing our agreements.

Our Customers are separate controllers of personal information we receive from them, and it is their obligation as controllers to determine their own retention periods. They may hold personal information for longer than we do.

Data Security

Our practices and processes are designed to protect the data that we process from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access using appropriate administrative, physical and technical security measures.

Profiling

We use personal information, such as attribute information, geographic location, network properties and user behavior data, sent by our Customers in order to produce various scores. Some of this data is collected by our Customers and passed to us through ThreatMetrix cookies and similar technologies that our Customers place or run on their Clients’ devices.

Our scores can be used by our Customers to predict the risk associated with a given transaction. Low confidence scores can suggest identity credentials being used fraudulently/out of prior context. Low trust scores detect unusual behavior, such as location anomalies, abnormally high number of new email addresses originating from the same device, or new shipping addresses that haven’t been seen before.

Our Customers configure their use of our services to address their unique needs, which may result in different scores among different Customers. Our services provide a platform for processing and applying rules to data but do not recommend to our Customers whether to take any actions based on scores. For the Clients, this means that Customers may make decisions that may affect online activity such as prohibiting access to a website, allowing an online transaction to proceed, or requiring a Client to provide additional authentication data. We do not make any decisions about an individual. Such decisions remain for our Customers to make.

Locations of Processing

We process personal information where ThreatMetrix and RSG companies and their service providers maintain servers and facilities, including in Iceland, the Netherlands, the United Kingdom and the United States. We take steps, including through contracts, intended to ensure that the personal information continues to be protected wherever it is located in a manner consistent with the standards of protection required under applicable law.

ThreatMetrix has certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce. Please view these entities’ Privacy Shield Notice here. To learn more about the Privacy Shield program, and to view these entities’ certification, please visit www.privacyshield.gov.
Your Rights

You have the right under European and certain other privacy and data protection laws, as may be applicable, to request free of charge:

- access to and correction or deletion of your personal information;
- restriction of our processing of your personal information;
- object to our processing; and
- the portability of your personal information.

If you wish to exercise any of these rights, please contact us at the address below. We will respond to your request consistent with applicable laws. To protect your privacy and security, we may require you to verify your identity. Where we are acting as a processor on behalf of our Customer, we will redirect you to make your request directly to our Customer.

Changes

We will update this processing notice from time to time. Any changes will be posted on this page with an updated revision date. If we make any material changes, we will provide notice through the services or by other means.

Contact

If you have any questions, comments, complaints or requests regarding this processing notice, please contact us online here for US requests or here for non-US requests. Alternatively, you can write to: Data Protection Officer, LexisNexis Risk Solutions Group, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, United Kingdom. You may also lodge a complaint with the data protection authority in the applicable jurisdiction.