ThreatMetrix Processing Notice

Last updated: May 15, 2018

About This Processing Notice

ThreatMetrix, Inc. (“ThreatMetrix”), a LexisNexis Risk Solutions 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. Your use of the ThreatMetrix website and other services is governed by the ThreatMetrix Privacy Policy.

Information Processed

Our organizational customers choose which personal information of their clients and prospective clients to send to us, such as names, mobile phone numbers, email addresses, mailing addresses and device identifiers. This information is immediately and automatically tokenized upon receipt, matched across different customers’ submissions throughout ThreatMetrix’s network of organizational customers, and combined into a unique digital identifier: the “ThreatMetrix ID”.

We also process personal information linked to the ThreatMetrix ID in a pseudonymous form, including, but not limited to: the number of email addresses and phone numbers associated with a client’s or prospective client’s Internet-connected devices; activities and attributes associated with a client’s or prospective client’s email addresses, shipping addresses, phone numbers, IP addresses; 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; client account details, log-in activity and history; and client transaction history associated with hashed credit card numbers, tracked over time, together with associated risk scores created or used by us through use of the services (collectively, ‘attribute information’).

Purposes and Legal Basis for Processing

We process such 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 similar laws.

Information Recipients

We share attribute information:

- with our customers and our processors;
- 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, our users, 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.

LexisNexis®
RISK SOLUTIONS

Data Retention

We retain personal information for only as long as necessary to provide the service and fulfill the transactions our customers have requested, 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.

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 attribute information, geographic location, network properties and user behavior data sent by our customers in order to produce scores such as the ThreatMetrix Confidence Score and the ThreatMetrix Trust Score. 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' and prospective clients' devices.

Our scores can be used by our customers to predict the reputational integrity of an ID for 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 ThreatMetrix to address their unique needs, which may result in different scores among different customers. ThreatMetrix provides a platform for processing and applying rules to data but does not recommend to its customers whether to take any actions based on scores. For our customers' clients and prospective clients, this means that ThreatMetrix's 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. Decisions remain for our customers to make.

Locations of Processing

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

Where personal information is transferred from the European Economic Area or Switzerland to a country that has not received an adequacy decision by the European Commission, we rely on appropriate safeguards, such as the European Commission-approved Standard Contractual Clauses and EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, to transfer the data.

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. For more information, see the ThreatMetrix Privacy Shield Notice. To learn more about the Privacy Shield program, and to view the ThreatMetrix certification, please visit https://www.privacyshield.gov/list.

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 Service or by other means.

Contact

If you have any questions, comments, complaints or requests regarding this processing notice, please contact: Data Protection Officer, LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, United Kingdom, DPO@lexisnexisrisk.com. You may also lodge a complaint with the data protection authority in the applicable jurisdiction.