



Ethoca's vision is to eradicate losses due to fraud and other types of unwanted customer-not-present transactional activities. Ethoca accomplishes this by powering a Global Fraud-Fighting Community ("Community") in which the members of the Community use their combined experiences to collaborate against fraud and other types of unwanted activity.

The Ethoca Code of Fair Information Practices

Ethoca understands that respecting the privacy of the data that has been entrusted to Ethoca is of paramount importance to the success of the Global Fraud Fighting Community.

Ethoca is therefore dedicated to maintaining the accuracy, confidentiality, security and privacy of all such data.

Ethoca therefore operates in accordance the Ethoca Code of Fair Information Practices ("Ethoca Code"). The Ethoca Code formally states the principles Ethoca follows in protecting and respecting the Private Information (defined below) in Ethoca's care. The Ethoca Code has specifically been developed, and is adhered to, in a manner that meets and exceeds industry best practices with respect to privacy.

Ethoca will continue to review the Ethoca Code on, at least an annual basis, to make sure it remains current with changing technologies, laws and evolving needs of the Community.

Scope of Applicability

The Ethoca Code of Fair Information Practices ("Ethoca Code") applies to data entrusted to Ethoca by members of the Global Fraud-Fighting Community while actively participating in the Global Fraud Fighting Community ("Private Information"). This includes all transaction data that is passed to Ethoca for evaluating or for use in evaluating the risk-of-loss associated with any transaction.

For the avoidance of doubt and without limitation, the Ethoca Code does not apply to data that is provided to Ethoca by members of the Global Fraud-Fighting Community (the "Community") that is not provided as part of their participating in the Community. This includes items such as, business terms between Ethoca and the member, business contacts of the Member, or business related communications between the member and Ethoca.



The Ethoca Code of Fair Information Practices (the “Ethoca Code”) has been drafted to be in agreement with the AICPA/CICA Generally Accepted Privacy Practices. It incorporates the ten principles defined therein. Ethoca’s practices as contained in the Ethoca Code are found below.

Principles and Practices

Principle 1 – Management

Ethoca maintains a privacy program which has been constructed in conjunction with the AICPA Generally Accepted Privacy Principles. Specifically:

- Ethoca maintains internal privacy controls to ensure that data cannot be accessed nor used for any purposes other than as necessary to assist the Community’s fight against fraud and other types of unwanted transactional activity, and to reduce Community Members losses attributable to such activity (collectively the “Allowable Uses”). Allowable Uses includes, but is not limited to:
 - Using historical transaction activity to evaluate the risk of fraud of a transaction currently being attempted.
 - Using the collection of data elements associated with a given transaction for the purposes of evaluated the risk of fraud associated with a transaction currently being attempted.
 - Using velocity of activity attributable to the various data elements of a given transaction to evaluate the risk of non-payment associated with a transaction currently being attempted.
- Ethoca’s privacy program is administered by Ethoca’s Chief Privacy Officer and all Employees are educated as to Ethoca’s Privacy obligations.
- Ethoca has engaged a third-party auditor to audit Ethoca’s compliance with the Generally Accepted Privacy Principles.
- Ethoca is registered as a Data Processor with the Irish Data Protection Commissioner.



Principle 2 - Notice

Ethoca works with Members to help ensure that the Private Information provided to Ethoca has been collected in a manner that provides adequate notice to the Community Members customers (“Customers”) of the manner in which their data will be used by the Community. Specifically:

- All members of the Global Fraud-Fighting Community agree to specific Terms of Use in which they are obliged to ensure that adequate notice is given to Customers in the transaction process that the Customer-provided transaction data may be used for the Acceptable Uses.

Principle 3 – Choice and Consent

Ethoca works with Members to help ensure that all Private Information provided to Ethoca is done with the appropriate knowledge and consent of a Customer. Specifically:

- Ethoca provides Community members (Members) sample consent language, appropriate to their jurisdiction, that can be used in their transacting processes.
- No community member is required to send any data to Ethoca for which appropriate consent has not been obtained.
- Participation the Community is entirely voluntary.

Principle 4 – Collection

Ethoca works with Members to help ensure that the information is collected by fair and lawful means and Ethoca limits its use of information collected to the Allowable Uses. Ethoca only collects information that is relevant for the Acceptable Uses.

Principle 5 – Use and Retention

Ethoca does not use or disclose the Private Information for purposes other than the Acceptable Uses. Further, Ethoca ensures that the collaboration it empowers is done so in manner that does not allow Members access to any Private Information that a given Member has not provided to the Community. Ethoca retains information only as long as necessary for the fulfillment of those purposes. Specifically:



- **Community members, at all times, maintain control the data they have provided to Ethoca.**
- **Ethoca acts on any instruction of a Member with respect to the Private Information the Member has provided to Ethoca.**
- **If a Member leaves the Community, all the data provided to Ethoca by the Member will be destroyed, removed or returned to the Member and will no longer continue to be utilized by the Community.**
- **Ethoca performs ongoing analysis of the data such that data is not kept beyond the date of its effectiveness in supporting the Allowable Uses. Data that is no longer required to support the Allowable Uses will be destroyed.**
- **Members of the Community are contractually bound to only use the information they receive from their participation in the Community for the Allowable Uses.**

Principle 6 – Access

Ethoca makes readily available to Community members and Customers information about its policies and practices relating to the Private Information and facilitates resolution of disputes to the accuracy of any Private Information held by Ethoca. Specifically:

- **Ethoca has a formal Dispute Resolution Policy that Community Members follow in the outworking of any Customer dispute with respect to the Private Information. The Dispute Resolution Policy is administered with the Member as the first line of communication with the Customer but provides for direct communication between Ethoca and the Customer in resolving any disputes. The Dispute Resolution Policy has been developed to facilitate full, reasonable, and clear disclosure of information to the Customer while continuing to ensure that the Member never has access to any Private Information that the Member has not provided to the Community.**
- **Community Members cannot obtain any Private Information that has been submitted to Ethoca by any other member.**



Principle 7 – Disclosure to Third Parties

Disclosure of Private Information in all instances is limited to the minimum required to support the Acceptable Uses. Specifically, this may include to a company or individual employed by Ethoca to perform functions on its behalf, such as research or technical support, consulting or auditing firms. In no event will such disclosures be made to any party with any less data protections than Ethoca has in place and only under contractual terms that strictly limit the disclosure for Acceptable Uses.

Ethoca will also disclose Private Information where such disclosure is required by law.

Principle 8 – Security for Privacy

Ethoca protects personal information by security safeguards appropriate to the sensitivity of the Private Information. Specifically:

- Private Information is labelled with the highest degree of sensitivity within Ethoca and, as such, is stored and transferred with the strictest safeguards that Ethoca employs.
- Ethoca is Payment Card Industry (PCI) compliant, is audited to the PCI standard each year, and is registered as PCI compliant Service Provider to the Payment Card Industry. All Private Information is handled in accordance with the PCI standard.
- Ethoca maintains its technology and business processes in strict compliance with the Ethoca Information Security Policy.
- The Ethoca Information Security Policy is reviewed and updated at least annually to help ensure that Industry best practices are always being utilized.

Principle 9 – Quality

Ethoca has instituted a Data Integrity Verification Program which has been developed to help ensure that the Private Information provided to Ethoca by Community Members is accurate. In the outworking of this program Ethoca works with members of the Community to identify any suspect information and correct any inaccuracies as required.

Principle 10 – Monitoring and Enforcement

Ethoca has a coordinated program in which it monitors its compliance to the Ethoca Code and Community members to the Terms of Use. Specifically:

- Ethoca has engaged third party auditors to audit Ethoca’s ongoing compliance with the Ethoca Code.
- Appointed a Chief Privacy Officer who is responsible internally for strategic oversight and coordination of Ethoca’s privacy protection and compliance efforts. The Chief Privacy Officer is responsible for:
 - Promptly relaying any credible evidence of or reports concerning violations of Ethoca Codes or security policy or law to the appropriate investigative authorities.
 - Providing information as necessary to Community members and Employees about existing and emerging legal and compliance requirements with respect to privacy and related best practices.
 - Ongoing notification to Community members and Employees about privacy policy and any revisions to the existing policy.
 - Supporting security and privacy awareness and education program efforts.
 - Supporting the monitoring and enforcement of privacy and security policies, and adoption of and adherence to best practices.
 - Supporting the development, implementation, and maintenance of information systems security and privacy policies and procedures where required in various areas, units, and functions in the business operation.
 - Acting as an advocate for budget and resource requests related to ensuring the maintenance effective information privacy and security programs.
 - Ensuring that appropriate audit services and reporting are in place to detect violations and to evaluate the effectiveness of privacy and security policies and of compliance activities.

Community Members and Customers may address any challenges or questions concerning Ethoca’s compliance with the Ethoca Code to privacy@ethoca.com.

page 6 of 6

Ethoca™ is a registered trademark of Ethoca Limited.

Board of Directors

Andre Edelbrock, President and Chief Executive Officer,
Executive Director
Darryl Green, Chief Operating Officer, Executive Director
John Fielding, Non-Executive Director

Joseph J. Grano Jr., Non-Executive Director

Tom Ridge, Non-Executive Director
Philip Nelson, Non-Executive Director
Hon. John D. Reynolds P.C., Non-Executive Director

Ethoca Limited
Denshaw House
120-121 Baggot Street Lower
Dublin 2
Ireland

Main: +353.1.469.3730
Fax: +353.1.469.3130

Ethoca Technologies Inc.
Suite 202
4211 Yonge Street
Toronto, ON
M2P 2A9
Canada

+1.416.849.6091
+1.416.849.6095