REFER.COM SECURITY, PRIVACY, AND ARCHITECTURE

Last Updated: August 15, 2015

Refer.com's Corporate Trust Commitment

Refer.com is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services ("Customer Data").

Services Covered

This documentation describes the architecture of, the security and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the services Refer.com provides ("Refer.com Services").

Third-Party Infrastructure

The infrastructure used by Refer.com to host Customer Data submitted to the Refer.com Services is provided by a third party provider, Amazon Web Services, Inc. ("AWS"). Currently, the infrastructure hosted by AWS in Provisioning of the Refer.com Services is located in the United States.
Additionally, a portion of customer support for the Refer.com Services is provided using third party technology (Infusionsoft) for secure storage of our client's contact information, and credit card information.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Refer.com Services:

Refer.com operates in an ITAR (International Traffic in Arms Regulations) Certified Facility as overseen by the US State Department and all employees are trained and tested at least annually on ITAR requirements and procedures requiring among other things security of data, company know-how, technical capabilities and facility. These guidelines are designed to protect company data from capture by foreign governments and other entities hostile to the United States and thus provide corollary benefits for the protection of sensitive data from incursion by other outside entities as well.

A PCI Compliance Audit and Certification is conducted on an annual basis by Trustwave as required by certain financial institutions with which Refer.com does business. These audits concern the security of sensitive customer data of all sorts, but also including credit card data. Refer.com is currently certified to be in full Compliance with PCI standards.

Additionally, the Refer.com Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

Security of Data Overview

We recognize that all client data, including contact details and correspondence is confidential. This recognition manifests itself in two major ways within Refer.com: 1) Strict internal procedures limiting and controlling our employee's access to client data. Beyond these procedures, password protections and other usual measures, all of our employees are required to sign a Secrecy and Confidentiality Agreement which we enforce and which is binding upon them; and 2) We utilize state of the art security procedures to protect our data bases within an Amazon Cloud solution.

Security Controls

The Refer.com Services include a variety of security controls. These controls include:

- Unique user identifiers (user IDs) to ensure that activities can be attributed to the responsible individual;
- Password length controls;
- Password complexity requirements for Web and mobile access to the Refer.com Services;
- Web and mobile access to the Refer.com Services via OAuth;

Security Procedures, Policies and Logging

The Refer.com Services are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a salted hash format and are never transmitted unencrypted;
- User access log entries will be maintained, containing date, time, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address. Note that source IP address might not be available if NAT(Network Address Translation) or PAT (Port Address Translation) is used by a customer or its ISP;
- Logs will be stored in a secure centralized host to prevent tampering;
- Passwords are not logged under any circumstances;
- No defined passwords are set by Refer.com;
- OAuth tokens are encrypted and not transmitted unencrypted.

Intrusion Detection

Refer.com, or an authorized independent third party, will monitor the Refer.com Services for unauthorized intrusions using network-based intrusion detection mechanisms. Refer.com may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Refer.com Services function properly.

Security Logs

All systems used in the provision of the Refer.com Services, including firewalls, routers, network switches and operating systems, log information to their respective system's log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

Refer.com maintains security incident management policies and procedures. Refer.com promptly notifies impacted customers of any actual or reasonably-suspected unauthorized disclosure of their respective Customer Data by Refer.com or its agents of which Refer.com becomes aware to the extent permitted by law.

User Authentication

Access to the Refer.com Services, directly or via the Refer.com API, requires a valid user ID and password combination, or an API key/secret, both of which are encrypted via TLS while in transmission. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Production data centers used to provide the Refer.com Services have systems that control physical access to the data center. These systems permit only authorized personnel to access secure areas. The facilities are designed to withstand any adverse weather and other reasonably predictable natural conditions, are secured

by around-the-clock guards, physical access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup

All networking components, load balancers, web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Refer.com Services is stored on a primary database server that is clustered with a backup database server for redundancy. All Customer Data submitted to the Refer.com Services is backed up daily.

Viruses

The Refer.com Services do not scan for viruses that could be included in attachments or other data uploaded into the Refer.com Services by customers.

Data Encryption

The Refer.com Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Refer.com Services, including 256-bit TLS Certificates and 256-bit AES encryption at a minimum.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data, to the extent such Customer Data can be copied and exported from the Refer.com Services and the ability to export such data is generally made available to customers, by contacting support@refer.com.

Deletion of Customer Data

After contract termination, to request deletion of Customer Data submitted to the Refer.com Services, contact us at support @refer.com. After such deletion is initiated by Refer.com, Customer Data will remain in inactive status on back-up media for 90 days, after which it will be overwritten or deleted. This process is subject to applicable legal requirements. Without limiting the ability for customers to request return of their Customer Data submitted to the Refer.com Services, Refer.com reserves the right to reduce the number of days it retains such data after contract termination. Refer.com will update this Refer.com Security, Privacy, and Architecture Documentation in the event of such a change.

Sensitive Personal Data

Important: The following types of sensitive personal data may not be submitted to the Refer.com Services: government issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life; information related to an individual's physical or mental health; and information related to the provision or payment of health care. For clarity, the foregoing restrictions do not apply to financial information provided to Refer.com for the purposes of checking the financial qualifications of, and collecting payments from, its customers, the processing of which is governed by the Web Site Privacy Statement for the Refer.com Services.

Tracking and Analytics

Refer.com may track and analyze use of the Refer.com Services for the purposes of security and helping Refer.com improve both the Refer.com Services and the user experience in using the Refer.com Services. Refer.com may also use this information and users' e-mail addresses to contact customers or their users to provide information about the Refer.com Services. Without limiting the foregoing, Refer.com may share data

about Refer.com customers' or their users' use of the Refer.com Services (“Usage Statistics”) to Refer.com’s service providers for the purpose of helping Refer.com in such tracking or analysis, including improving its users’ experience with the Refer.com Services, or as required by law.

Interoperation with Other Refer.com Services

The Refer.com Services may interoperate with other services provided by Refer.com which are subject to these same Refer.com Security, Privacy and Architecture policies.