Fraud.net

FACT SHEET

Security and Compliance

Fraud.net maintains a robust and comprehensive multi-level security environment which is mapped against the highest levels of industry compliance.

CERTIFICATIONS

HIPAA COMPLIANT

UNITED STATES DEPARTMENT OF COMMERCE NTIS National Technical Information Service

PCI DSS COMPLIANT

AICPA SOC

DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA

EU GDPR COMPLIANT

SECURITY

Fraud.net operates on, and believes in, extreme trust principles. Customer trust is of paramount importance to us. To that end, all customer data stored by Fraud.net is protected by industry best practices that are continuously monitored and carry strong administrative and operational procedures. To achieve the high levels of data protection required by our customers, Fraud.net maintains a robust and comprehensive multi-level security environment which are mapped against the highest levels of industry compliance. We are a 100% cloud-born service provider encompassing highly sensitive data sets. Therefore, our security measures are also heightened to meet the sensitivity of the data.

Here are some of the best practices we deploy:

PHYSICAL SECURITY

Fraud.net leverages virtual compute nodes on Amazon Data Centers (AWS) in multiple locations meeting local data retention, jurisdictions or laws. All of Amazon data centers exhibit strong physical security measures exceeding or meeting best industry practices and are under constant compliance objectives of government, healthcare and other sensitive business sectors. Amazon data centers provide 24×7 surveillance, including keycard and biometric access controls to the facility. Furthermore, all of Fraud.net's office locations are also under 24×7 surveillance and badged, though it is a bit redundant control. By design, Fraud.net operates its offices and remote locations (Enterprise Network) as untrusted entities warranting stronger segregation and access requirements to Amazon production facilities, which houses core sensitive data sets.

DATA PROTECTION

Fraud.net adheres to and deploys strong data protection policies and procedures while maintaining its compliance with GDPR, HIPAA, PCI-DSS SAQ.D and customer obligations. By design, no PII (Personally Identifiable Information) or sensitive data is allowed to leave the controlled production environment, which is totally segregated from non-production and Enterprise network by design. So any sensitive data never actually leaves Amazon production premises. If required, all PII or sensitive data sets are obfuscated first prior to leaving the production environment into non-production for any testing

and development functions. Data scrubbings are fairly well defined functions minimizing human interactions, though production data access also comes with tightly defined RBAC (Role Based Access Controls), and all access are secure logged, tamper proof, and monitored in real time for any potential abuse or unauthorized access. Real-time monitoring on sensitive data sets includes any abnormal behavior or usage and is manned by our 24×7 staff members, along with tightly integrated incident management processes.

DATA ENCRYPTION

Fraud.net uses industry best practices to safeguard data in transit or at rest. TLS is mandated and enforced for all sensitive transactions between the end-points, and AES 256 bit encryption is used to protect data at rest for each customer with unique keys in a multi-tenant environment on Amazon. GDPR, HIPAA, SOC2 Type II, PCI-DSS SAQ.D, C5 Frankfurt, etc. compliance levels are enforced on our sensitive data sets meeting the highest regulatory and trust principles across continents. A strong Key Management System (KMS) is in place issuing proper key rotations and management practices. Risks to data hostage situations have been accounted for while maintaining strong key management practices such as issuing, rotating, or revoking keys when an employee leaves or role changes, along with key backups for emergency and BCP (Business Continuity Planning) scenarios. The KMS also comes with strong role segregation principles where key creation, substitutions, and or changes are completely segregated from key users, be it a human or machine.

USER AUTHENTICATION

Each user on Fraud.net environment has a unique username. We offer forms-based authentication (username and password) and second factor (Google Authentication) to all users of Fraud.net, along with SSO integration authentication for compliance with any corporate authentication or identity management policies for the underlying services. Fraud.net supports complex password policies and it is customizable by each customer meeting their own password complex policy requirements. Fraud.net issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include either the user name or password of the user. Fraud.net does not use cookies to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs. All account login attempts are logged, and account lockout policies are automatically applied after a certain number of failed login attempts.

OPERATIONAL MANAGEMENT

We have implemented policies and procedures designed to ensure that your data is secure and backed up to multiple physical locations, or selected locations meeting local laws and jurisdictions. Our team is continually evaluating security and operational threats and implementing updated countermeasures designed to prevent unauthorized access to or unplanned downtime of the API services. Access to all Fraud.net production systems and data is limited to authorized members of the Fraud.net Technical Operations team, who go through rigorous training and awareness, along with background check procedures. In addition, Fraud. net has strong well defined operational controls in the following realms:

CHANGE MANAGEMENT

Fraud.net maintains a change management process to ensure that all changes made to the production environment are applied in a deliberate and controlled manner. Changes to information systems and other system components are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended. Fraud.net has version controls and can reverse the applied changes, should an unknown error were to be encountered.

VULNERABILITY MANAGEMENT

Fraud.net has tightly integrated SDLC (Software Development Life Cycle) procedures along with continuous vulnerability assessment and management programs. Fraud.net is 98% serverless architecture, and any code, mainly 'functions' on AWS go through rigorous testing and quality assurance along with their OWASP Top 10 built in code scanning checks during software development phases. Any high or critical vulnerability findings are fixed as spotted, and non-criticals are allocated to be fixed as per their risks and time factors. Each vulnerability is reviewed to determine if it is applicable, ranked based on risk, and assigned to the appropriate team for remediation. Strong SDLC is a requirement in meeting compliance levels of PCI-DSS explicitly, and it scales to other compliance expectations as well, which Fraud.net adheres to as explained previously. Fraud.net contracts with third-party security professionals to conduct network and application penetration testing annually to proactively find new attack vectors and security weakness.

PATCH MANAGEMENT

Fraud.net operates on 98% serverless architecture, and due to which has a tremendous reduced patch operating environment. It is almost non-existent for practical purposes. The core infrastructure patching responsibilities (Operating Systems, Networks, and related physical components) reside with AWS or Amazon. In few OS instances (EC2), Fraud.net deploys a robust patch management process, meeting 100% critical patch uptime. Thereby, Fraud.net adheres to 100% critical patch compliance objectives by default on a nightly or daily basis.

SUPPLIER AND VENDOR RELATIONSHIPS

Fraud.net partners with suppliers and vendors that share similar values around lawfulness, ethics, integrity and best practices. As part of our third party due diligence and review process, we screen our suppliers and vendors and bind them to appropriate confidentiality and security obligations, especially if they manage or handle customer or sensitive data.

Our procurement department may perform audits from time to time on Fraud.net's suppliers and vendors in an effort to ensure the confidentiality, integrity, and availability of data that our third-party suppliers or vendors may handle.

AUDIT AND ASSURANCE

Fraud.net maintains a cloud-based tamperproof centralized logging platform for real time alerting and analytics. These logs provide a full history of who, what, when and where accountability factors across all of our core offerings. Access to our auditing and logging tool is controlled by limiting access to authorized individuals. Security events are logged, monitored, and addressed by trained security team members on a 24×7 basis. Organizational responsibilities for responding to events are defined and tightly coupled with our incident management procedures (see below). All logs come with well defined retention policies and procedures.

Furthermore, all administrative access to data, information, file attachments, images, PII, and other content that is uploaded or submitted to customer instance of the API Service on Fraud.net infrastructure are reviewed on a quarterly basis by internal auditors to confirm that we use it only for the purposes permitted by the agreement governing your use of the Fraud.net service.

As part of its proactive defense posture, Fraud.net also has a Bug Bounty program and encourages ethical hackers to identify bugs and get rewarded.

CONTINUOUS MONITORING & INCIDENT MANAGEMENT

Fraud.net has a formalized incident response plan (Incident Response Plan), continuous monitoring and associated procedures in case of an information security or outage incidents. The Incident Response Plan defines the responsibilities of key personnel and identifies processes and procedures for notification. Incident response personnel are trained, and execution of the incident response plan is tested periodically.

An incident response team is responsible for providing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

BUSINESS CONTINUITY AND DISASTER RECOVERY

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, we implement a BCP or Disaster Recovery program at all our data center locations. This program includes multiple components to minimize the risk of any single point of failure. For business critical applications, application data is replicated to multiple systems within the data center and, in some cases, replicated to secondary or backup data centers that are geographically dispersed to provide adequate redundancy and high availability. Data retention or jurisdiction obligations are never breached while meeting local laws in such plans.

DISCLOSURE

Fraud.net maintains a policy of full event disclosure for security incidents that affect customer data. In the event of any security incident affecting your data, a notification will be sent to your account administrator. Fraud.net additionally publishes information about the health of our service on our customer portal dashboard.

ENGAGEMENT

If you find a security issue with our products or if you are concerned or suspect that your Fraud.net account has been compromised, please contact us at security@fraud.net or call us directly at (866)-971-2030.

CHANGES

We may update this Security Statement as we add new security capabilities and make security improvements to our services. If we make any significant material changes, we will notify you via email prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our security practices.

v1.3 – Oct 1, 2021