First AML

Security Posture

First AML is committed to being a trusted partner for compliance by following industry best practices and achieving key security certifications. Our security-first culture translates into reduced risk and peace of mind for both our clients and their customers alike.

Ethos

In today's environment, breaches happen. The key is to have in place robust security systems that can identify, protect, detect, respond and recover from breaches with minimal impact.

With this context in mind, at First AML we focus heavily on Data Loss Prevention (DLP), ensuring we can:

- detect breaches and the exfiltration of sensitive data in a timely manner, to reduce the level of impact.
- block the attempt before significant harm occurs.
- respond quickly and appropriately to any breach, including: board-level down governance, detailed incident response/business continuity processes and committed response timeframes with relevant and accurate impact information.
- identify (log, audit and alert) specific data that has been compromised thereby identifying end users / customers who are impacted and mitigating the need to widely announce a breach.

First AML platform overview

First AML is an all-in-one AML platform. It powers thousands of compliance experts around the globe to reduce the time and cost burden of complex and international entity KYC.

Our enterprise-wide, long term approach to the CDD data lifecycle addresses time and cost challenges while improving the customer experience and minimising reputational and security risk. The First AML platform includes the following key features:

- Auto KYB entity unwrap / build
- Manifest case management hub
- Verification and identity configurations
- Public API + embedded EIV
- Risk assessments
- Screening / continuous monitoring
- KYC / KYB / KYS
- Reporting

Contents

This whitepaper outlines First AML's company and platform security posture including:

Security Architecture and Infrastructure

Secure engineering practices

First AML's security posture combines secure engineering practices with trusted, external validation. In addition to industry standard processes (such as using the principle of least privilege, ensuring continuous monitoring and incident response, utilising encryption and data protection methods) we also utilise or ensure:

- Penetration tests conducted three times a year
- Threat modelling
- Adherence to secure coding standards (based on OWASP)
- A regularly reviewed, secure software development lifecycle
- Automated patching and updates on a regular basis
- Configuration management (including validating best practices on configuration items)
- Secure third-party integrations
- Proactive cloud security management
- Defence in depth - starting with engineer education and supported by a range of tooling.

Data security

All data transmitted and stored via the First AML platform is encrypted both in transit and at rest using the industry standard AES-256 encryption algorithm to encrypt data. All data in transit utilises TLS 1.2+ encryption. Access to customer data is highly secured and audited.

All First AML issued devices have full disk encryption, anti-virus / anti-malware protection and can be remotely wiped. All cloud storage is encrypted, private by default, and is continually monitored for changes in configuration that could expose data. For further information on data security refer to the First AML data processing addendum.

Secrets management

All secrets and sensitive configurations are stored and encrypted in AWS. Only a small subset of senior on-call engineers have the ability to view and modify this information.

Network security

Network segmentation is applied to prevent guests, who are provided WiFi access, to access any resources on the First AML internal network.

All public facing production systems utilise web application firewalls to protect against malicious traffic and requests.

Anomalous network activity is automatically identified, logged and will raise alerts 24x7.

Authentication and Access Control

First AML issues employee system access on a least privilege basis, and reviews internal user access on a quarterly basis. All production access is audited and logged for review and forensic analysis. Access is revoked when no longer needed.

Additional access controls include:

- Multi-factor authentication (MFA) enforced for all production access
- Access to production AWS systems are limited to authorised Site Reliability Engineers and on-call staff only
- Comprehensive audit logging of all access attempts and actions
- Session expiry after period of inactivity
- Ability to remotely revoke access if credentials are compromised

Data Storage and Retention

Data centre security

First AML production data and systems are hosted in Amazon Web Services (AWS) data centres, and physical security is managed by AWS at the Perimeter, Infrastructure, Data and Environmental layers.

Examples of AWS security features leveraged by First AML include:

- Use of accounts, security groups, web application firewalls, and VPCs to isolate environments
- Automated detection of insecure configurations or suspicious activity
- DDoS protection to mitigate distributed denial of service attacks
- Regular backups, versioning, and geo-replication for disaster recovery

Additional information on AWS Data Centre physical security can be found on the AWS Data Centres site.

Data retention

We will retain Personal Information (for a full description, please reference the personal and sensitive data section of this document):

1. for as long as necessary to achieve the purposes for which it was collected; or
2. in some cases, where we have an ongoing legitimate need to do so (for example, to comply with legal, tax or accounting obligations, or to resolve disputes), for longer than is necessary to achieve the purpose for which it was obtained.

When we no longer have an ongoing legitimate need to process Personal Information, we will either delete or anonymise it. If deletion or anonymisation is not immediately possible (for example, because the Personal Information has been stored in backup archives), we will securely store the Personal Information and isolate it from any further processing until deletion or anonymisation is possible.

For further information on data storage and retention refer to the First AML data processing addendum.

Suppliers

All of First AML's suppliers undergo a security and legal review prior to being engaged. Suppliers are monitored on an on-going basis with annual and ad-hoc reviews as required.

Software suppliers have an added layer of scrutiny where we place a heavy emphasis on companies that, where possible:

- Practise continuous integration/continuous deployment (CI/CD), ensuring they can quickly respond and patch emerging vulnerability issues.
- Conduct anomalous network behaviour monitoring, especially in CI/CD or build environments that have wide reaching permissions.
- Themselves have strong internal vendor selection and review processes to ensure their entire supply chain is adequately secured.
- Understand the importance of SBOM (software bill of materials) monitoring to understand the full landscape of direct and indirect dependencies (and their related vulnerabilities).

Reliability and Availability

First AML has a Site Reliability Engineering team and on-call engineers to provide 24x7 support for platform issues and incidents. All production systems provide resiliency (providing multi-availability zone and regional redundancy for disaster recovery scenarios).

First AML utilises the following AWS regions for delivering its service:

- APAC: primary region: ap-southeast-2 (Sydney) with us-west-2 (Oregon) for disaster recovery scenarios.
- EU: primary region eu-west-1 (Ireland) and eu-central-1 (Frankfurt) for disaster recovery scenarios.

Security Monitoring and Incident Response

Logging and monitoring

First AML leverages industry standard tooling to provide 24x7 monitoring of all production systems. Anomalous behaviour and activity is automatically identified and alerted upon. All platform events and activity are securely logged, with up to a year of retention to assist with analysis and forensics. Audit logs for all customer specific platform operations are securely stored for the lifetime of that customer.

Vulnerability management

All operating systems, dependencies and container images are continuously scanned using best-in-class tooling, and vulnerabilities addressed in accordance to severity and impact.

Developers are made aware of potential vulnerabilities early in the software development lifecycle, to ensure remediation early. A database of scanned components provides the ability to identify new and critical zero-day vulnerabilities as soon as they are released

Incident response

In the event of a Security Incident, First AML shall:

1. notify Customer without undue delay and in any event such notification shall, where feasible, occur no later than 48 hours from First AML becoming aware of the Security Incident;
2. provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and
3. promptly take all reasonable steps to contain, investigate, and mitigate any Security Incident. First AML's notification of or response to a Security Incident under this Section 6.3 (Security Incident Response) will not be construed as an acknowledgment by First AML of any fault or liability with respect to the Security Incident.

For further information on security monitoring and incident response refer to the First AML data processing addendum.

Compliance and Certifications

ISO 27001

First AML maintains ISO 27001 certification, the international standard for information security management systems (ISMS).

The scope of the certification includes: Information Security Management System covering the design, development, testing, deployment, operations and support of First AML Limited (NZBN: 9429046463005), First AML PTY Limited (ABN:643929140), and First AML UK Limited (number 13802565) Anti-Money Laundering solutions including personally identifiable information (PII), through global business activities in accordance with the Statement of Applicability version 2.0 dated 17/10/2023.

First AML is audited every twelve months as part of our ISO27001 certification requirements.

Employee Training, Policies and Procedures

Training

First AML employees undergo criminal background and reference checks prior to commencing employment. All employees are required to accept our information security policies, and acceptance of these are recorded and reported against. All staff undergo security awareness training including secure development training for our software engineers.

Ongoing security awareness training covers data protection, access controls, social engineering, phishing, and more.

Policies

First AML has a number of robust security policies and procedures in place. All staff are trained during induction and on an ongoing basis to ensure continued familiarity and compliance.

First AML's security related policies and procedures include but are not limited to:

- An Information Security policy which is maintained, reviewed and signed off annually and with changes communicated to staff.
- All legislative statutory, regulatory and contractual requirements are documented and kept current for all information systems and are communicated to staff.
- Role termination controls with detailed steps taken when someone leaves the organisation.
- Controls to prevent unauthorised use of equipment which could be used to access client data.
- Controls to protect unauthorised access or loss of client information to which First AML employees may have access.

Customer Responsibilities

First AML expects customers to undertake their own data loss prevention (DLP) measures in helping to identify and prevent unsafe or inappropriate sharing, transfer, or use of sensitive data.

Accuracy, quality, and legality of customer personal data

In addition, customers are solely responsible for the accuracy, quality, and legality of their customer personal data and the means by which they acquire said data. Customers represent and warrant that:

1. It has provided, and will continue to provide, all notice and obtained, and will continue to obtain, all consents, permissions and rights necessary under Data Protection Laws for First AML to lawfully process Customer Personal Data on Customer's behalf and in accordance with its instructions;

2. It has complied with all applicable Data Protection Laws in the collection and provision to First AML and its sub-processors of such Customer Personal Data; and
3. It shall ensure its processing instructions comply with applicable laws (including Data Protection Laws) and that the processing of Customer Personal Data by First AML in accordance with the Customer's instructions will not cause First AML to be in breach of applicable Data Protection Laws.

Customer security advice and guidance

Based on industry best practices, First AML recommends clients protect their systems and data by following standard security procedures:

- Only hold data as long as needed. Excessive data acts as a breach impact multiplier.
- Move inactive client data to secure storage off-network and hold only as long as needed for audit reasons.
- Utilise network segmentation to create secure zones and minimise potential breach impact.
- Ensure all software is supported and patched.
- Review and amend warnings/alerts to minimise fatigue, ensuring people act.
- Enforce end-to-end hardware encryption (e.g. laptops) to minimise the attack surface
- Review privileged access to systems.
- If running in-house created software utilise secure coding practices and employ regular external penetration testing.
- Utilise application allow lists, permitting only authorised software to run on your network.
- Focus heavily on minimising account compromise. Accessing systems through legitimate entry points such as a compromised login is much easier than finding other avenues of compromise for attackers such as vulnerable software or networks.
    - Practise mature identity management practices - both internally and across your vendors:
- Utilise pass keys where possible
- Centralise identity management/single sign-on (SSO)
- Utilise IDaaS (Identity as a Service) providers to handle authentication, reducing vulnerability management overheads. IDaaS are significantly targeted by security researchers and are more likely to have vulnerabilities identified and fixed vs. home-grown or less popular solutions.
- Enforce MFA for staff, vendors and suppliers
- Identifying indicators of account compromise (such as impossible travel, unknown network addresses etc.) and alerting/responding in a timely manner is key to reducing losses related to account compromise. Key partners should have suitable alerts and robust monitoring in place.

- Social Engineering
    - Compromising individuals and/or physical security of buildings is far simpler and more effective. Consider these attack vectors and how they can be made more secure.
    - Provide initial and ongoing security training and education to staff.
- Consider and understand the evolving world of AI and machine learning.
    - Technologies such as LLMs/Generative AI have unlocked a wide range of new capabilities, and opened up a significant number of new (and yet to be discovered) attack vectors. For more information on this, read our recent article, "What happens when generative AI can spoof biometrics."

Office Security

First AML physical offices have restricted entry, protected with badge reader access controls, and security cameras at entry points. All visitors must sign in, be escorted by First AML staff, and are restricted to common areas only. Office work areas are restricted to staff members only, with no visitor access permitted.

For further information on office security refer to the First AML data processing addendum.

Disaster Recovery and Business Continuity

As part of First AML's ISO 27001 certification, business continuity processes are audited. The First AML Business Continuity and Disaster Recovery programme is validated throughout the year, including activities intended to reduce platform recovery time.

Database snapshots are taken multiple times a day, plus continuous backups with a 5-minute restore granularity to ensure recovery of data with as little data loss as possible. Uploaded files and documents are stored in a versioned write-only manner, with documents continuously replicated to another region to provide regional redundancy for disaster recovery scenarios.

Data Protection and Privacy

The First AML platform meets relevant local legislative requirements in regards to the collection, storage, processing, and handling of user data.

Data protection policy and procedures

Data protection officer (DPO)

First AML employs a dedicated DPO, ensuring that personal data is processed in a lawful, transparent, and secure manner.

Data protection regulations

First AML complies with relevant privacy legislation within the United Kingdom, New Zealand, Australian, and European countries (GDPR). Full information on our GDPR compliance can be found at the link.

Personal and sensitive data

Personal and sensitive data stored on the First AML platform include:

- First and last name
- Email
- IP address
- Device ID
- Domain server
- Type of device/operating System, browser used
- Photos/selfies
- Videos
- Gender
- Residential address
- Date of birth/age
- Digital images
- Recordings of environment or documents provided by clients of customer
- Identity documents
- Country of residence and location data
- Country of citizenship
- Tax number
- Forms, information and documents required for tax reporting purposes (e.g. financial statements, trust documents, FATCA/CRS status, info and/or returns)
- Other documents provided by the clients of Customer