



Payments Compliance and Risk Programs

Rippling places Compliance and Risk at the forefront of its payment operations, recognizing the complex and ever-evolving legal, regulatory, and operational aspects of payroll and payments processing. Key to this is Rippling's continued effort to hold and maintain relevant licenses in markets which it operates and to work with similarly licensed partners.

Rippling compliance programs are based on global payment regulatory rules, guidance and best practices that often exceed regulatory requirements governing payment processors. Rippling's policies and programs are approved by the licensed Rippling entities' management and are available to Rippling employees.

Anti-Money Laundering and Sanctions Program

Our AML program utilizes a risk-based approach to monitor and mitigate the inherent risks with our unique product offerings and customer portfolios. The program is designed to detect and prevent money laundering and terrorist financing activity on the Rippling platform and ultimately provide the safest environment for our customers.

Internal policies

Relevant compliance policies, including the AML Policy and AML Risk Assessment, are reviewed annually and approved by the regulated entity's Board of Directors. Program and procedure documentation providing more detailed information on operational standards is maintained by the first line and Compliance team, and is internally restricted to protect sensitive information as needed.

Compliance officer

The Compliance program is overseen by global and local Board-appointed Compliance Officers, with experience in payments and financial transactions compliance.

Training

Rippling conducts annual AML/CFT, sanctions, and risk training for all employees working on payments-related products, including targeted team training focused on specific risks that vary by function. The training program is developed and delivered to ensure all staff are sufficiently knowledgeable to identify and escalate any suspicious activity.

Customer due diligence

Rippling maintains a robust Know Your Customer (KYC) program (also known as a Customer Due Diligence program), which includes enhanced due diligence procedures designed to understand customer risk profiles and provide a greater level of scrutiny where appropriate.

Fraud and Credit Risk Management

Robust fraud detection and risk mitigation measures are essential to ensuring a safe and healthy payments and payroll platform and overall financial ecosystem. To this end, Rippling has developed and runs a prevention, detection, and investigation program to identify and control credit, fraud, and operational risks, with the goal to protect our customers, their employees, and our partners from bad actors.

Customer identification verification

Risk mitigation and fraud prevention start with customer onboarding. At Rippling, customers are required to provide critical KYC information at onboarding. Rippling utilizes this information, internal tools, and leading providers of authentication and verification services to manage the risk of identity fraud on our platform.

Transaction monitoring

Rippling maintains a robust detection program to systematically monitor its regulated activity for anomalous or inconsistent data and outliers for both credit and fraud purposes. Additionally, Rippling leverages custom transaction monitoring rules based on known money laundering and terrorist financing typologies targeted at payment processors and payroll providers.

Sanctions Program

Rippling maintains robust policies and procedures to ensure that company services are not utilized by, or on behalf of, sanctioned parties. As part of this program, Rippling maintains a continuous monitoring system to ensure that changes to relevant sanctions lists are updated daily and that customers, employees, and contractors are screened against this list at onboarding and on an ongoing basis. Rippling also utilizes technical controls and blocks products to prohibit payments to countries that are under a comprehensive sanctions program. Rippling's sanctions program is reviewed at least annually and approved by the Board.

Regulatory Complaints Handling

Rippling maintains a structured complaints handling framework to ensure compliance with applicable regulatory requirements and to protect the integrity of its financial services. This framework provides a clear process for receiving, documenting, investigating, and resolving complaints in a timely and transparent manner. Rippling's Compliance team oversees complaint management, ensuring root causes are identified and remedial actions are implemented to prevent recurrence. In addition, Rippling tracks and reports complaint trends to management and regulators as required, with the objective of promoting accountability, maintaining customer trust, and continuously improving its compliance and risk programs.

Safeguarding

Rippling is committed to maintaining robust safeguarding arrangements to protect customer funds and ensure compliance with global regulatory standards. As a global payments and payroll provider, Rippling ensures it complies with all local rules regarding the protection of client funds. Ensuring they are held with reputable financial institutions in accordance with local client fund safeguarding requirements. The safeguarding framework ensures that customer funds are fully protected in the event of insolvency, operational disruption, or other adverse events. This program is reviewed regularly to ensure continued adherence to regional regulations and alignment with international best practices, reflecting Rippling's commitment to transparency, trust, and the protection of customer assets worldwide.

Audit Programs

Rippling believes a robust payments and payroll Compliance and Risk program must include independent assessments of key policies, procedures, and other controls. To this end, Rippling leverages experienced independent auditors specializing in fintech compliance to review and assess Compliance and Risk programs on an annual basis.

Anti-money laundering and sanctions audit

Rippling's AML and sanctions programs are independently assessed on an annual basis. These reviews test the overall integrity and effectiveness of the AML and sanctions systems, controls, and compliance with applicable laws and regulations.

Key annual audits include:

- **Fraud and risk audit:** Rippling's Fraud and Risk program is independently reviewed each year to test the maturity and strength of Rippling's fraud and credit risk controls, including the effectiveness of prevention and detection controls.
- **Nacha audit:** Rippling's ACH Program is reviewed annually to ensure that all processes are executed in compliance with the Nacha Operating Rules, the governing organization of the ACH Network. This audit includes a review of our compliance policies and framework, information security policies, and other operational procedures relevant to the creation, transmission, and return of ACH files with partner institutions.