Corpay Cross-Border

# Data Privacy & Security Overview

Corpay is a leading provider of integrated cross-border payment services and risk management solutions. Moreover, as a trusted service provider, Corpay delivers innovative solutions designed to mitigate foreign exchange exposure and address unique business needs. Our award-winning capabilities and industry-leading technologies simplify the way businesses connect with the global marketplace.

Corpay is committed to securing and protecting our clients' data. Each jurisdiction we operate in has different requirements. Our privacy policies provide details:

https://payments.corpay.com/privacy-policy
You may also contact privacy@fleetcor.com

The following is a summary of the measures we take to protect the privacy and security of client data. Our approach matter is multi-faceted, involving physical, technical and preventative measures.

## Data Protection and Privacy

We have physical access controls in place to ensure our facilities are secure. Our data centres and offices are only accessible to authorized personnel.

- Corpay's data centres are equipped with many enterprise-class physical and environmental controls, including backup generators, uninterruptible power supply, redundant HVAC systems, 24/7 onsite security and cameras.
- Remote offices have access to our core platforms exclusively through a firewall that is routed through our secure virtual private network (VPN). Likewise, remote access to Corpay's network is protected by multi-factor authentication.
- Our technological architecture integrates control mechanisms: financial, operational, data processing and logical. These are all designed to help protect our – and our clients' – assets and information. Corpay's online platform session management and access controls ensure data segregation on a customer by customer basis.
- Corpay's online platforms are only accessible via secure channels using HTTPS encryption to ensure the protection, integrity and privacy of the data.
- We follow agile software development lifecycles, meaning we make continuous updates to Corpay's platforms. We practice secure coding: we test all our software releases, and have a change control process in place, thus ensuring continuous and quality product releases.

— Our corporate email service includes features such as high-availability and enterprise email security to protect against email-based cyber threats such as spam and malware. Also, for emails containing financial, personal or otherwise sensitive details, we use encryption services.

Corpay is committed to upholding the applicable data protection standards under the European Union's General Data Protection Regulation (GDPR); likewise, under California's California Consumer Privacy Act (CCPA). These rights include, as applicable:

— GDPR sets limits on when we may transfer personal data to a country outside the European Economic Area lacking EU-equivalent privacy protection.

— Subject to recordkeeping laws such as anti-money laundering laws, GDPR and CCPA each create the right for a data subject to ask us to return and/or erase (and/or correct, in some circumstances) personal data we have regarding the data subject.

— Corpay has insurance coverage for network security/ privacy liability. That policy has a group limit of USD $10 million. This coverage is subject to possible change (by our parent company FleetCor) from time to time.

## Information Security

— Corpay's dedicated information security team, led by Corpay's ISO (Information Security Officer), identifies and responds to cyber security threats. The team also performs security risk assessments and tests the ongoing adequacy of our security measures. These measures are critical to our security protection, awareness, reporting processes and programs.

— Corpay takes a defense in depth approach to protect the integrity of information systems through multi-layered security counter measures.

— We have intrusion detection and prevention solutions in place to ensure protection against reconnaissance and intrusion attempts targeted at Corpay's data centers.

— We protect against advanced persistent threats and malwares using an advanced malware protection system.

— We protect ourselves with a sophisticated threat detection and response platform backed by a 24/7/365 monitoring team.

— Corpay has also implemented a Web Application Firewall to monitor traffic and secure its applications.

— Corpay conducts regular vulnerability scanning, along with annual external penetration testing and application security evaluation. All findings are reviewed by our information security and technology teams. We also conduct re-testing as part of the external penetration and application security testing engagement. With these steps we resolve any findings and protect information systems and applications against known vulnerabilities.

— We review and assess the security of our online platform on an ongoing basis to make sure the environment is continuously updated and protected from new security threats.

— We have an information security incident response process in place (including an incident to ensure timely response to any information security incidents.

## Reliability

— Our critical systems technology platform is designed with enterprise-class information systems. These systems have high availability architecture, ensuring quick response times, resiliency and scalability.

— Our core data centre is set up with redundant internet connectivity through multiple internet service providers over high- speed fiber circuits. We also use an advanced Border Gateway Protocol routing setup to ensure internet services are protected and to maintain high availability.

— Corpay utilizes multiple managed DNS service providers to maximize availability and protect against denial-of-service attacks.

— We host online systems using technology that incorporates full redundancy and load balancing.

— Our critical databases run on a distributed enterprise database system platform hosted on high-availability infrastructure with automatic failover capabilities.

— Our technology operation teams use a platform which constantly monitors all critical systems. This monitoring enables us to both quickly identify any performance or systems alerts and efficiently respond and resolve the issues underlying such alerts.

## Regulatory and Audits

- Obligations to FINTRAC, FinCEN, AMF, AUSTRAC, ASIC, MAS, FCA, and Central Bank of Ireland as well as numerous state regulators, including business conduct standards and meeting financial condition requirements measured by capital and liquidity thresholds.
- Licensed and regulated in all operating jurisdictions from both product and anti-money-laundering perspectives. Registered as an investment company in Australia, Singapore, the European Union and the United Kingdom.
- Americas: Licensed as a Money Services Business (MSB) in the United States and Canada under FINCEN and FINTRAC, respectively.
- APAC: The Australian practice is a Financial Services Licensee (AFSL) under the Australian Securities & Investment Commission (ASIC). The Singapore operation is licensed and regulated as a Remittance Business and a Capital Markets solutions provider under the Monetary Authority of Singapore (MAS).
- EMEA: UK companies are licensed as an E-Money licensee and a Derivative Investment Company through the Financial Conduct Authority (FCA) in the UK. We are authorised as a Payments Institution and as an investment firm by the Central Bank of Ireland and deemed authorised in the European Union under MiFID.
- Subject to external financial, compliance and technology security audits, led by a globally recognized firm, in all jurisdictions in which it operates on an annual basis.
- We engage independent external auditors annually to conduct audits of our processes and controls. Conducted audits include SSAE 16 SOC1 Service Organization Control Audits, Risk Assessments, and Compliance audits. Our annual audits include detailed testing of the controls we have in place to conduct foreign exchange transactions.
- Corpay periodically undertakes a SOX audit. We undergo a successful SOC1 Type 2 audit once every year.

## Transaction Processing

- Corpay's proprietary payments and trading platform and accompanying systems are built in-house, and are designed and wholly owned by Corpay.
- Transactions are processed through Corpay's in-house systems.

Data are stored at our primary and secondary data centres – all located in Canada. This means the data are protected by the Canadian privacy laws which the European Union has recognized as "adequate": that is, substantively as protective as GDPR.

- We take multiple measures to protect confidential data, and the information systems hosting this information, throughout their lifecycles.

## Business Continuity

- All critical databases are replicated continuously to our standby data centre located in Canada.
- We also follow a robust data backup process through which we securely backup data to encrypted offsite storage.
- Our Disaster Recovery and Business Continuity Plan takes into account foreseeable events that may disrupt service in all of our global offices. If the disruption in local service takes place for an extended time period, Corpay can leverage other Corpay offices to minimize the impact on our customers.
- Corpay utilizes a third-party disaster recovery planning and recovery service. We regularly conduct disaster recovery testing and remediation of disaster recovery test findings. This way we are prepared in case of a disaster recovery situation.

The foregoing is a summary and is subject to change. Corpay continues to invest in cutting-edge technologies and infrastructure improvements that both support our financial services and secure our industry leadership now and into the future. If you require further information, please contact us directly at info@corpay.com.

Corpay

Corpay.com