spenda

Security FAQ's

www.spenda.co

Contents

Contents

Contents

Q. What measures does Spenda have in place to ensure compliance with Anti Money Laundering (AML) and Know Your Customer (KYC) laws and regulations?

At Spenda, we have several measures in place to ensure compliance with Anti Money Laundering (AML) and Know Your Customer (KYC) laws and regulations.

These include:

1. Conducting thorough background checks on all new customers and partners to ensure they are legitimate entities.
2. Keeping up to date with the latest AML and KYC regulations, laws, and best practices, and ensuring that our policies and procedures are in line with them.
3. Training our staff on AML and KYC requirements, laws, and regulations so they can identify and report any suspicious activity. We take AML and KYC compliance very seriously at Spenda, and we strive to ensure that our customers' transactions are conducted in a safe and secure manner.

Q. What is the purpose of Anti Money Laundering (AML) and Know Your Customer (KYC) laws and regulations in Australia?

KYC is the process of obtaining information about a customer and verifying their identity. AML is a complex of measures carried out by financial institutions and other regulated entities to prevent financial crimes.

These laws prevent illegal money activities by detecting and reporting suspicious financial actions like money laundering and financing terrorism. They protect and maintain the stability and honesty of the Australian financial system.

Q. How does Spenda make sure customer data is safe? What specific security measures do you have in place?

Spenda implements Two Step Authentication as an additional security measure to safeguard your data and prevent unauthorised access. We have also integrated an AutoSave function that allows you to pick up where you left off and an automatic log out security measure which helps to keep your account secure.

Q. What is Two Factor Authentication, and how does it add extra protection to your account?

Two Factor Authentication is a security process that adds an extra layer of protection to prevent unauthorised access to your account. With Two Factor Authentication, you need to provide two forms of identification to log into your account. Firstly, you enter your Spenda username and password, and then you will need to provide a second form of identification, either a code sent to your mobile via text message, or a security token sent to your chosen authentication app.

Q. What accounting software is Spenda currently compatible with, and do you offer custom integrations?

At present, Spenda is compatible with Xero, MYOB, and QuickBooks. Our team frequently incorporates new integration partners and can also provide custom integrations.

Q. What measures does Spenda take to ensure that business transactions are created and stored securely, and how do these measures ensure the protection of sensitive information?

Spenda has a range of measures to ensure that business transactions are created and stored securely, leaving no room for potential vulnerabilities. To safeguard the privacy of our users, Spenda adheres to the relevant privacy laws and regulations governing the collection, storage, retention, and deletion of personal information.

Q. How does Spenda maintain the security of user data, and what specific measures do you take to identify and address potential vulnerabilities before they occur?

To maintain the security of user data and ensure compliance with regulations, Spenda regularly conducts security assessments through both internal and third-party assessors. This helps us to ensure your data is kept safe and transactions always remain compliant.

Q. What is Payment Card Industry (PCI) compliance and why is it important for credit card transactions in the payments industry?

PCI compliance is a global standard mandated by the leading Card Schemes including Visa, MasterCard and American Express to reduce the risk of card data breach and to help ensure the security of credit card transactions in the payments industry. Spenda undergoes regular annual PCI compliance checks and is currently PCI compliant.

Q. What is an annual PCI compliance review?

PCI (Payment Card Industry) compliance is a set of industry standards that businesses must follow when handling credit card information. An Annual PCI compliance review ensures that a business is following the necessary security protocols to protect credit card information. This is done by PCI QSA (Qualified Security Assessor) a third party authorised assessor that performs the annual review as per PCI guidelines and validates the businesses compliance.

Q. How does Spenda prevent fraud?

Spenda uses services such as 3D Secure, which ensures that the cardholder and authoriser is whom they claim to be. This helps reduce the liability to the merchant for any fraudulent transactions.

Q. What measures are in place to ensure the security and privacy of communication with Spenda and third-party entities, as well as the restricted access to data by authorised users?

All communication between Spenda, third-party organisations and individuals are encrypted with industry standard SSL/HTTPS. These are security technologies that help keep your personal information safe and private when you're using the internet by encrypting the data that's being sent between your computer and the website.

Q. I'm concerned about providing my credit card details. How does Spenda keep my credit card details protected?

All credit card details are saved using a method called 'tokenisation' that keeps personal data secure. Spenda's tokenisation replaces your credit card details with a unique token that is only usable within your Spenda account. This way, we don't need to store your credit card details in our system, maximising your security.

Q. What measures does your organisation take to ensure that all staff, board members, and executives are trained on security and privacy matters?

All staff, board members and executives undergo regular security and privacy training to ensure we keep up to date with the everchanging cyber security landscape.

Q. Who has access to my data?

At Spenda, we have implemented a zero-trust model, which means only authorised individuals are able to access certain information based on their position in the organisation.

Regular comprehensive internal and external penetration testing and vulnerability scanning is performed on all our systems by trusted third party security vendors.

Q. What does Spenda do with old or redundant user data?

As per industry security and privacy standards, we delete and destroy all data that is no longer needed.

Q. What is the purpose of using risk assessment reviews at Spenda, and how do they help in maintaining the security and privacy of the organisation's operations?

The purpose of using risk assessment reviews at Spenda is to identify and evaluate potential security and privacy risks to the organisation's operations. By doing so, we can identify areas of vulnerability and take proactive steps to prevent security breaches or privacy violations.

Q. What steps does Spenda take to ensure the security and reliability of your build and deployment pipeline, and how does this allow you to confidently and efficiently upgrade your Spenda Systems while delivering more value and functionality to your customers?

Our build and deployment pipeline are peer reviewed and secured to ensure only approved changes are deployed to our system. We also have a large, automated test suite to ensure a high level of automated security and regression testing. This, combined with our regular and frequent release cycle, allows us to confidently and efficiently upgrade our systems should vulnerabilities or security risks arise as well as delivering more and more value and functionality to our customers.

Q. What are Spenda doing with the capital until they move it on NPP via Zepto?

Funds are held in the inter-bank clearing system and then Zepto / Spenda clearing accounts for less than 1 minute. The funds are in transit and managed by the system. They cannot be used or touched whilst in transit.

Q. Do Spenda provide risk guarantees in the event of default, fraud, or insolvency?

Spenda is an audited, regulated entity that must keep cash balances in excess of A$2m at all times. Our solvency would not affect a Carpet Court trading period as the lead time between a solvency issue and Carpet Courts ability to terminate our agreement and prevent loss is at 60 days. In the event of default (administration), cash in transit would continue and be paid, as Spenda do not have access to the cash in transit. With respect to Fraud, Spenda are insured for such event and naturally it would depend on where the “fault” of the fraud lay e.g: member or Spenda.

Q. Reading the terms and conditions we also need to agree to Zepto's terms and conditions. Do Zepto also provide risk guarantees in the event of default, fraud, or insolvency?

Spenda have back-to-back agreements with Zepto for the provision of services. Like Spenda they are regulated and have minimum cash at hand requirements like other financial intermediaries. As with Spenda, Zepto's system requires compliance and certification audit to mitigate the risks of fraud and ensure that utilisation of funds across their ecosystem is in accordance with NPP, and ACH banking system requirements. Zepto as an intermediary do not hold funds, rather facilitate the transition of funds. In the event of failure on their behalf, the transmission would not occur, and funds would be returned to the originating party (the member).

Q. As an example, what would happen if CCA system was hacked, bank details changed, therefore members payments went to the wrong account. Who is accountable?

Bank details for transfer of funds from member to CCA are pre-defined (ie: entered by member) and required 3 layers of verification being achieved. To modify the payment destination a hacker would not only need to steal passwords to access the primary login to Spenda, but they would also need to steal the phone of a Carpet Court administrator to complete to two factor authentication, then they would need to impersonate a Carpet Court Administrator and complete the funding account request process and have this approved. *In the unlikely event that a hacker was able to do this accountability would sit with sit with Spenda or Carpet Court – depending on the nature and cause of the breach.* Current processing using a simple ABA file are less secure, for example, to beat an ABA file, a hacker simply needs to login to Xero or MYOB and change the destination account of any payee. It is uncommon to verify the destination of funds and there is no security on this data within these products or notifications at bank that the BSB and ACC information has been changed.

spenda

www.spenda.co