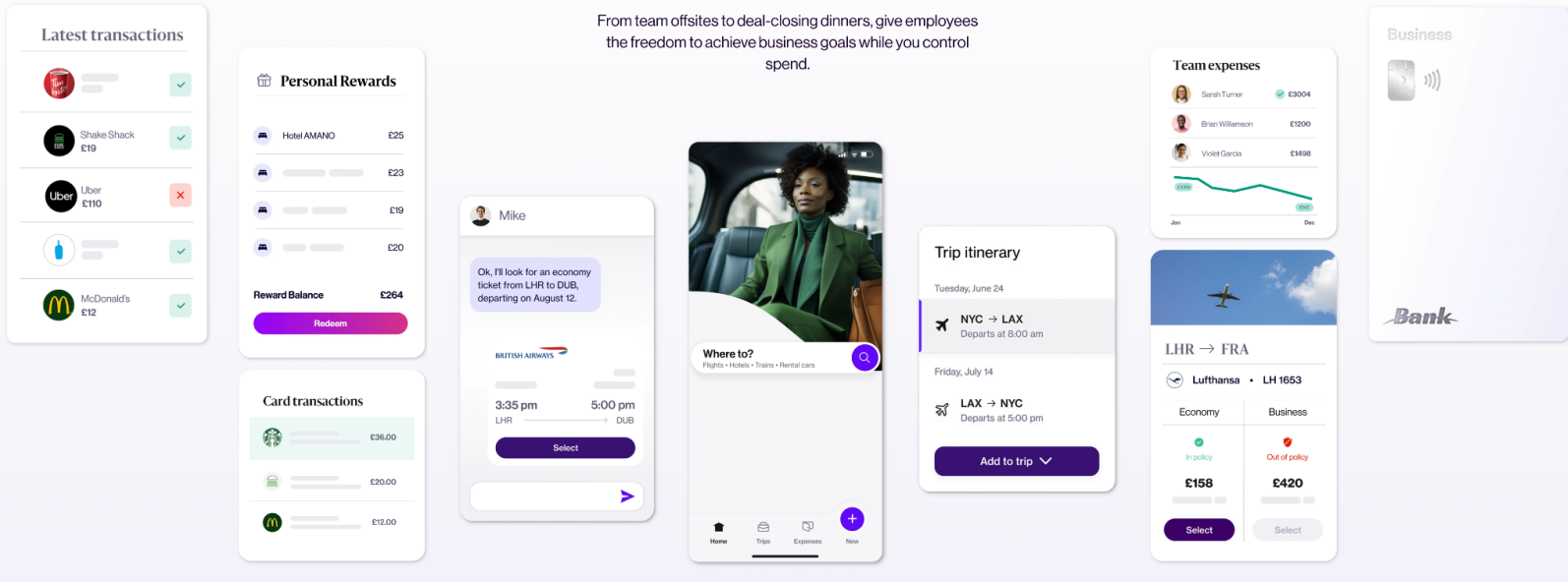


NAVAN

Generation Digital

Experience the all-in-one travel and expense platform

From team offsites to deal-closing dinners, give employees the freedom to achieve business goals while you control spend.



Everyone's travel and expense destination

Business Travellers

- ✈ Book and manage travel in one place
- ✳ Earn points from your favourite loyalty clubs
- 📅 Get Navan Rewards for personal trips
- 📄 Never file an expense report again

Travel Managers

- ✉ Invite employees and guests to book their own travel
- 🛡 Set spend guardrails so everyone stays within policy
- 👤 Enhance your duty of care by knowing where your travellers are
- 🏠 Make changes on Navan or with our 24/7 travel support agents

Finance & Accounting

- 📊 Automatically categorise and reconcile every expense
- 📅 Get full visibility into every expense in real time
- 🔗 Integrate key expense data with your ERP in seconds
- 🚩 Automatically flag out-of-policy transactions

Executive Assistants

- 📅 Book the perfect trip—your exec's favourite travel options are shown first
- ✍ Automate itinerary emails, calendar syncing, and loyalty accumulation
- 🛠 Easily change travel on your own or get help from experts 24/7
- 🏆 Earn Navan Rewards towards your personal travel

Pay Your Way

Payments

Optimize your T&E program for control and efficiency, no matter how your teams spend. Leverage Navan corporate cards, Navan Connect (compatible with Visa, Mastercard, and American Express corporate cards), and reimbursements for spending on personal cards.

Navan Connect partners with:  •  • 

Navan Expense

Spend smarter

Streamline your expense management from swipe to reconciliation. Automate categorisation, reports, and reimbursements. Boost productivity and optimise savings with AI-powered insights.

Navan Travel

Travel made easy

Build, manage, and scale your company's travel programme with ease. Empower employees to book from an extensive inventory while staying within your spending limits.

ISO



Security certifications

Navan maintains a formal and comprehensive security programme designed to safeguard against security threats or data breaches, prevent unauthorised access, and uphold the security and integrity of our customers' data. The specifics of our security programme are outlined in our third-party security audits and international certifications.

Regular audits by third-party assessors evaluate our internal controls, ensuring the protection of the security, confidentiality, integrity, availability, and privacy of the information our customers entrust to us.



Product security features



Application security

To help ensure the continued security of its applications, Navan's comprehensive Application Security program is intricately involved and integrated with its Secure Software Development Life Cycle (SDLC) process. The security team collaborates closely with the development team to incorporate security measures at every step of the SDLC, including annual penetration testing and regular application security testing as part of the CI/CD pipeline. Navan's website, microservices, and Application Programming Interfaces (APIs) regularly undergo vulnerability and penetration testing, security scans, threat detection, and security assessment testing conducted by cybersecurity professionals.



Detection and response

Navan's detection and response team is dedicated to threat-detection engineering, vulnerability management, incident response, and crisis communication management. Navan vigilantly monitors its production environments to identify and address any vulnerabilities that might compromise data security. Our comprehensive incident response plans and playbook ensure that security events are managed promptly and effectively, minimising impact and allowing business operations to return to normal swiftly.



Infrastructure and cloud security

Navan's platform and applications are hosted in [AWS cloud data centres](#) located across multiple regional availability zones. Our strategy for securing customer data leverages robust AWS security features, including Virtual Private Clouds (VPCs), Security Groups, the AWS Key Management Service (KMS), and more. [AWS data centre](#) facilities employ innovative secure architectural engineering methodologies, which are directly incorporated into the Navan platform and infrastructure.



Network security

Navan has established detailed operating policies, procedures, and processes designed to manage the overall quality and integrity of our environment effectively. We actively monitor network activity for anomalies 24/7 and respond to security events within minutes. In addition, we've implemented proactive security measures, including perimeter defence and network intrusion prevention systems (IPSs). These IPSs monitor critical network segments for atypical network patterns in the customer environment, as well as traffic between different service tiers.



Security governance

We consider our employees to be our first line and strongest defence against cyber threats. Our team receives regular training and updates on security education and best practices to drive awareness, reduce risk, and remain vigilant against potential threats. Ongoing application security training is mandatory for our developers, and Navan adheres to a multitude of industry best practices and recommendations, including those from the Open Web Application Security Project (OWASP) and other industry-standard control systems.



Encryption

Navan transfers clients' data using multi-layered security mechanisms, fortified networks, and Transport Layer Security (TLS) encryption for data 'in transit'. For sensitive data 'at rest' in storage, we utilise Advanced Encryption Standard (AES), the current industry standard for modern commercial business applications. We regularly review and update our encryption protocols, ensuring they continue to meet industry standards and effectively counter the latest encryption-breaking tactics.

