FINASTRA

Building a Secure Bacs Payments Process

The Cornerstone of Business Stability

Table of contents

Avoiding threats to your Bacs business

In the dynamic realm of payment processing, downtime is more than an inconvenience; it represents a profound threat to your business.

Picture this: during a payroll cycle, a payment processing system experiences a glitch, leaving employees unpaid and unable to make bill payments. A similar disruption when collecting recurring payments from customers may result in interruptions to cash flow, eroding business growth prospects and possibly damaging your company's reputation.

Scenarios like these underscore the critical importance of embedding resilience into the payments process and finding a strategic partner who can support your goals.

Operational resilience — the ability to quickly adapt to and recover from unforeseen circumstances, such as natural catastrophes, cyber incidents or power outages — is particularly important in the UK market, where Bacs serves as a primary method for making recurring electronic payments.

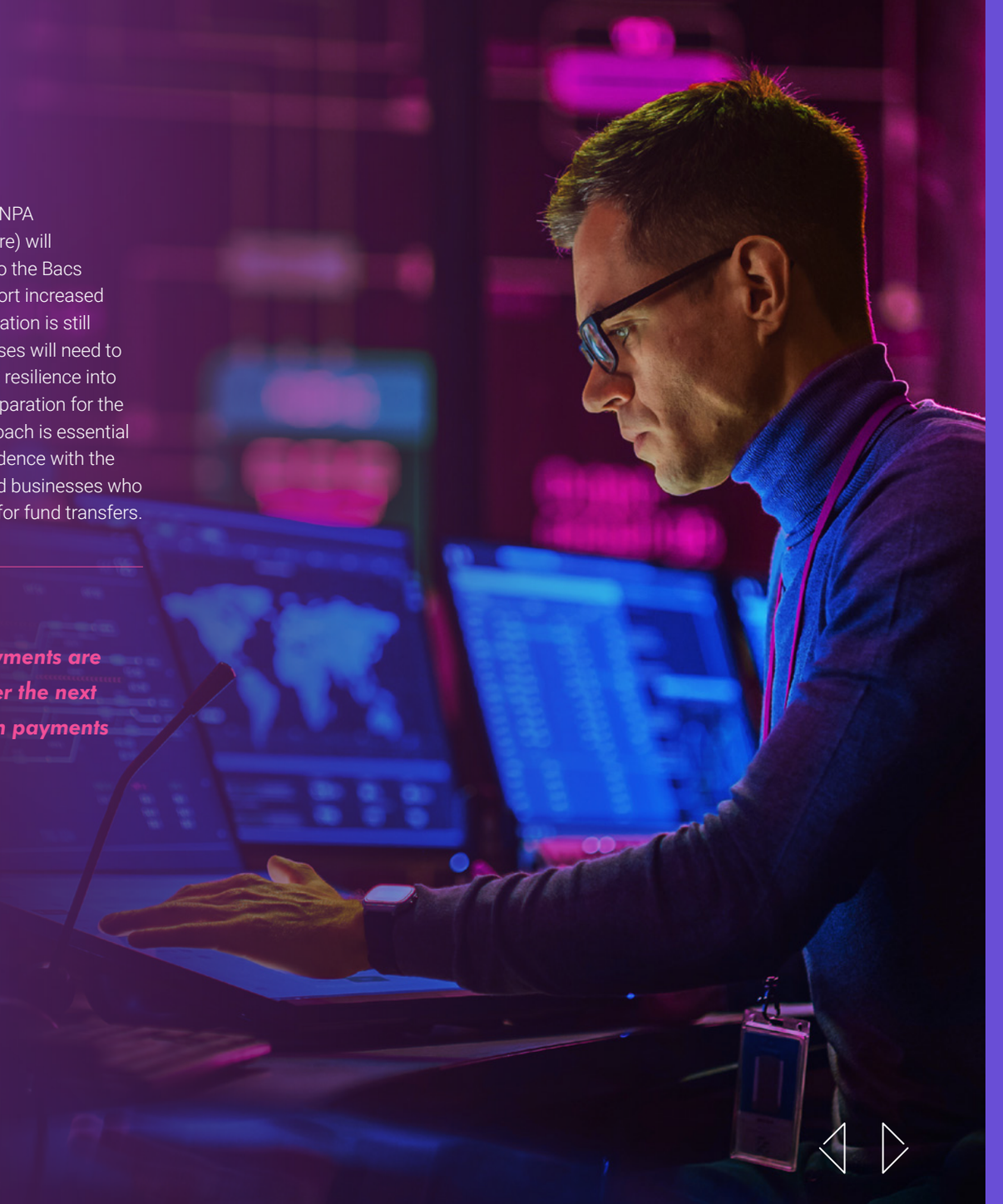
Limitations imposed by the Bacs scheme put companies at heightened risk when disruptions occur, especially when considering the increasing expectations for rapid or same-day processing:

- Payments take a minimum of three days to clear
- Bacs payments are not processed on weekends or bank holidays
- Bacs payments observe strict daily cut-off times, meaning your payments must be submitted in a timely manner for prompt processing

While these inherent restrictions underscore the importance of resilience in ensuring the timely flow of electronic payments, a look to the future only increases the emphasis. Bacs Direct Debit payments are expected to grow over the next decade, with 5 billion payments forecast in 2032.[1] Added payments create additional stress across the network, requiring organisations to anticipate a potential increase in disruptions and delays, while also preparing for a swift recovery.

The planned launch of the NPA (New payments Architecture) will bring necessary changes to the Bacs infrastructure to help support increased payments flows, but finalisation is still many years away. Businesses will need to embed enhanced payment resilience into their operations now in preparation for the changes. A proactive approach is essential to preserve trust and confidence with the consumers, employees and businesses who depend on these systems for fund transfers.

> ***"Bacs Direct Debit payments are expected to grow over the next decade, with 5 billion payments forecast in 2032."***



> *In a recent survey, 46% of CFO respondents indicated that payment automation reduced disputes and exceptions.*

Automation, the key to building a resilient payments process

When it comes to building a resilient payments process, automation is key. Automated payment solutions remove manual steps from invoicing through to approval and payment submission, reducing instances of error and improving process efficiency. In a recent survey, 46% of CFO respondents indicated that payment automation reduced disputes and exceptions,[2] a factor that can significantly streamline the payments lifecycle.

Reducing errors during payment processing also plays a critical role in mitigating overall organisational risk. Consider how easily an extra zero entered during a batch request could delay processing, impacting the company's relationship with its suppliers, customers or employees and potentially damaging its bottom line. Now consider how automating functions, such as adding Confirmation of Payee for bank account number and sort code validation checks, can reduce error rates associated with manual data entry, exposing the organisation to lower risk.

Automation also plays a role in improving employee productivity.[3] A recent survey revealed that 77% of workers feel they would be more productive if they could automate routine tasks.[4] Of the employees who use automation tools, 50% said they saved on average 3.5 or more hours per week.

While automation has many benefits, not all companies will want to automate end-to-end. Fortunately, leading payment solution providers build in flexibility, allowing organisations to determine where they will maintain manual steps and checks.

Considering the role automation plays in ensuring a streamlined payments process, finding a technology provider with the right attributes becomes critical to building resilient processes. Leading payment service providers offer versatility and integrity controls that minimise disruptions and help ensure maximum adaptability.

Finding a payments technology provider—security protocols are crucial

In a market as dynamic as the UK, prioritising resilience in the payments process is not just a matter of convenience. It's a fundamental necessity for maintaining the stability of electronic payments. In this environment, the security protocols offered by your service provider are vital to ensuring resilience at every level of your payments landscape.

More than 80% of individuals in the UK receive their wages through Bacs Direct Credit transfers, further underscoring the need for payments security.[5] But many companies continue to overlook security when assessing service providers. After all, their current provider must understand the criticality of keeping customer or employee data safe, or they wouldn't be in business.

However, leading providers stand apart from the rest by employing a key set of security attributes that augment resilience.

When evaluating your service provider or seeking a new relationship, it's vital to ensure the technology can deliver the following security capabilities:

Leading security standards

Adherence to the latest in security standards is critical to keeping data safe and ensuring prompt efficient transaction processing. Mature Information Security and Information Technology policies and processes must be coupled with a rigorous oversight program to ensure the defined security standards are met. Data centres used should be accredited to the relevant standards – some good ones to check for are ISO/IEC 27001 (Information Security Management System), ISO 22301 (Business Continuity Management System) and ISO 9001 (Quality Management System).

Cyber Essentials Certification is another key component that businesses should look for when evaluating payments providers. A Cyber Essentials certificate ensures that the provider meets minimum qualifications through a self-assessment. These include five technical controls: boundary firewalls and internet gateways, a secure configuration, access control, malware protection and patch management.

A Cyber Essential Plus certification adds weight to the Cyber Essentials certificate, through independent testing and assurance.

> ***"More than 80% of individuals in the UK receive their wages through Bacs Direct Credit transfers, further underscoring the need for payments security."***

Communication protocols

SFTP (Secure File Transfer Protocol) security protocols and API calls are powerful tools designed to securely transmit payment information, ensuring the confidentiality of sensitive financial data.

SFTP employs strong encryption and authentication mechanisms, creating a secure avenue for exchanging payment data, such as bank account details.

However, the advantages associated with API calls extend beyond secure data transmission, allowing organisations to receive data in return. This two-way communication allows for real-time monitoring of payments, enabling organisations to track the status of transactions, identify issues or discrepancies, and ensure payment integrity.

Additional security capabilities to consider

Disaster recovery and contingency plans

Do you know how your service provider would manage your payments if they experienced a critical server failure, perhaps due to a natural disaster? If the provider has a disaster recovery and contingency plan in place, your transactions will continue to sail through, thanks to careful forethought from your provider.

Disaster and recovery plans provide a structured framework for swiftly responding to disruptions, outlining the steps to take in emergency situations to minimise downtime and ensure the continuity of critical payment functions.

In a similar way, contingency plans protect the payments process by establishing preventive measures to mitigate the impact of identified risks. These plans encompass a wide range of scenarios, from technical glitches and security breaches to natural disasters and other disruptions.

Disaster recovery plans should also provide a roadmap for effectively managing each situation.

When it comes to implementing disaster and recovery plans, robust architecture is an essential component of a swift recovery. Ensuring access to capabilities, such as multiple data centres, backup power supplies, redundant internet providers and dynamic capacity management will support a swift response to challenges, reducing the likelihood of prolonged disruptions.

> ***"When it comes to implementing disaster and recovery plans, robust architecture is an essential component of a swift recovery."***

Single sign-on (SSO)

While a single sign-on capability is largely recognised as a mechanism for users to access multiple applications or systems, SSO credentials can also enhance the security of your payments process.

With SSO security in place, businesses can easily add or remove user privileges without logging into the connected systems, allowing for greater automation and standardisation of security. Companies can easily eliminate access to sensitive data, and also gain additional monitoring capabilities.

API calls

By utilising API calls, businesses can perform periodic checks of user activity and audits to help prevent fraud. This level of visibility and control not only safeguards the payments process but also streamlines security management, contributing to the overall efficiency and resilience of the organisation's financial operations.

Ensuring downstream security

While the security protocols enforced by your service provider offer critical controls when it comes to building a resilient payments operation, it is only one step in creating the adaptability your business needs to thrive. Organisations must also consider the resilience of downline systems, such as those used by customers receiving payments. The high-level standards employed by your service provider must also be replicated across each supplier or payment recipient.

> *"In a world where flexibility, security and adaptability are paramount, your payment solution provider becomes a strategic partner."*

Final thoughts on building resilience

No two businesses are alike, and neither are their payment flows. While many corporates may initiate a flurry of transactions at the beginning of the month and enjoy a more tranquil pace thereafter, others see a variety of transaction peaks and troughs.

Your payments provider should have experience in supporting all environments and the appropriate technology to ensure the best performance now and in the future. For instance, can your provider set you up with a single tenant Software-as-a-Service (SaaS) solution when your transaction processing needs accelerate beyond what is supported by your current setup?

While a multi-tenant environment may reduce your costs and efficiently handle several use cases, once you reach a certain level of transaction activity, single-tenant installations could improve processing flows, speed of data transfer and security.

The enhanced performance will provide greater resilience across your payments function.

In a world where flexibility, security and adaptability are paramount, your payment solution provider becomes a strategic partner, offering resilience against unforeseen challenges, and the ability to ensure seamless payments.

FINANCE IS OPEN

Finastra unlocks innovation across the world of financial services, through our trusted software and open platform.

About the author

Liz Carroll
Senior Product Manager

Liz has worked at Finastra for more than 20 years (starting originally with Accountis Europe, a startup in North Wales, now part of Finastra), joining to co-create their first Bacs product. She started her career as a software developer, but her passion for translating customer requirements into developer specs and quality software solutions, meant a move to product management was inevitable. With a keen interest in UK payments, Liz is the face of Finastra's Bacs business for corporate payment services.

Sources

1. "UK Payment Markets Summary 2023." UK Finance Sept 2023.
2. "Solving Accounts Payables' Top Frictions with Automation." PYMNTS, July 2023.
3. "State of Work, 2nd Edition." Slack from Salesforce, 2023.
4. "State of Work, 2nd Edition." Slack from Salesforce, 2023.
5. Pay.UK, https://www.bacs.co.uk/bacs-schemes/bacs-direct-credit/paying-by/

Contact us

About Finastra

Finastra is a global provider of financial software applications and marketplaces, and launched the leading open platform for innovation, FusionFabric.cloud, in 2017. It serves institutions of all sizes, providing award-winning software solutions and services across Lending, Payments, Treasury & Capital Markets and Universal Banking (Retail, Digital and Commercial Banking) for banks to support direct banking relationships and grow through indirect channels, such as embedded finance and Banking as a Service. Its pioneering approach and commitment to open finance and collaboration is why it is trusted by over 8,000 institutions, including 45 of the world's top 50 banks. For more information, **finastra.com**

Corporate Headquarters
4 Kingdom Street
Paddington
London W2 6BD
United Kingdom
T: +44 20 3320 5000

ID-40734 / 0324

FINASTRA