How to deliver card payments that are always PCI compliant

Overcoming the compliance challenges of IP-based card-present payment networks

Foreword

The world of payments is in a state of flux, with new payment methods, channels and market-altering competitors bringing considerable change. Card payments where the card holder is present have become the basis of the payment economy and are growing rapidly as people leave cash behind.

The pressure this puts on organisations to deliver a smooth, reliable and rapid card payment process is driving a shift to feature-rich IP-based payment services. However, organisations also know that connecting points of sale to the wider network increases the risk of a data breach – and every operator is well aware that non-compliance with the Payment Card Industry Data Security Standards (PCI DSS) can have serious consequences for the business.

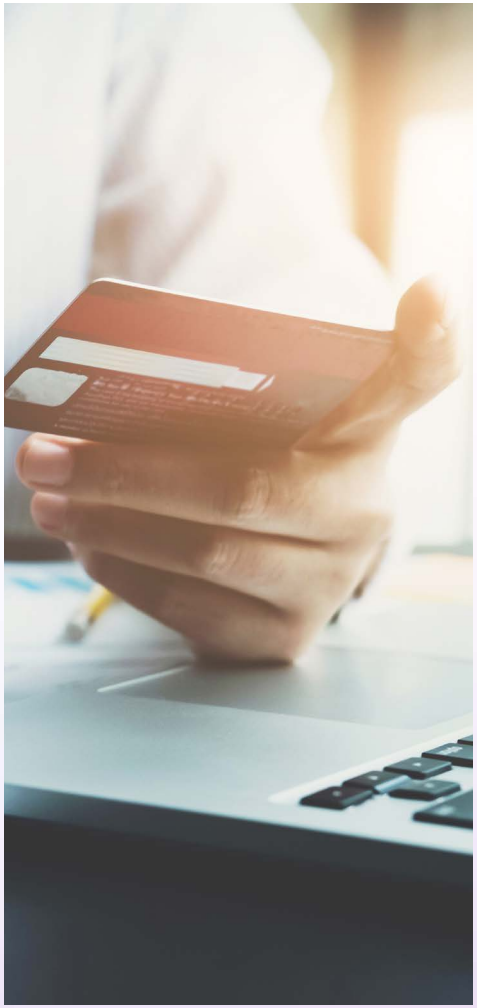
When I talk to customers, many know they need to evolve their payment strategy but are concerned about how to do it without making their lives more complicated and opening the door to regulation and compliance headaches.

How they navigate through this feels like a make-or-break moment. They want to seize the opportunity to make the most of payment technology to stay competitive, but can see potential difficulties with security, networks and PCI DSS compliance. Plus, they're aware that they need a solid and reliable networking base before they can add other payment technologies to their sites.

My conversations with forecourt operators, multinational franchise operators, multiple-site merchants and acquiring banks revolve around the need for simplicity and compliance in payment systems so, to help determine the best route forward, we've summarised the current market position in this eBook.

I hope it clarifies your strategic thinking around your payment systems, positioning you to ride the waves of payment evolution.

Marie Boycott,
Head of Payments, BT



This eBook will examine:

- the factors at play in the payment environment
- the PCI DSS compliance challenge
- what the ideal card-present payment system looks like
- how BT Cardway with Mako technology delivers an 'in a box' solution
- case studies of BT Cardway in action.

What's happening in the card payment world?

Since the pandemic, the global card and payments market has been shifting and the landscape is still evolving. Today, businesses of all sizes are revaluating their payment strategies to tackle the key changes emerging in the market:

1. An accelerating trend towards card payments and a cashless society

When large sections of the global economy, like high streets and physical retailers, were temporarily closed during the pandemic, it made card payments a popular option. However, what considerably accelerated the global trend towards card payments was people's unwillingness to touch cash or the terminal when in store.

Since then, this overwhelming shift has continued. Final figures for 2022 are expected to show that the global cards and payments market has grown from $763.2 billion in 2021 to $847.56 billion in 2022 – an annual compound growth rate (CAGR) of 11.1%. By 2026, this is expected to reach $1,269.23 billion at a CAGR of 10.6%.

In contrast, cash use is declining steadily. Even in traditionally cash-heavy environments, use of cash hasn't bounced back to the levels seen before the pandemic. In total, over 80% of retail spending across the UK now uses debit or credit cards.

2. Widespread growth in new payment points

The pandemic also accelerated the popularity of contactless and seamless, self-service payment models. Now, convenient payment options are becoming the expected norm for consumers across a range of services and these forms of transactions are likely to continue to increase in frequency.

A good example is the growing popularity of electric vehicles and their charging stations which primarily use electronic and app-based payments or tap-to-pay. As these environmentally conscious vehicles become more common, vendors will need to invest in more on-premise payment points and devices to service this need.

3. New market disruptors and innovators

In recent years, new entrants to the market like fintech organisations have intensified competition by directly challenging traditional banking models and payments services. Instead of traditional card-based transactions, these organisations are bringing a range of alternative payment methods to point of sale (POS) payments – such as the use of digital wallets that use mobile or app-based payments. Elsewhere, a host of new payment devices such as wearables like watches are springing up.

Payment technologies for an evolving market

The shift away from legacy technologies which used the old PSTN network, like X.25 dial terminals, has delivered innumerable benefits.

By leveraging the near ubiquity of wired and wireless broadband, the time taken to process transactions has reduced significantly. Rather than having to have a dedicated phone line for each payment terminal, many can share a single broadband connection, reducing costs for multi-lane merchants.

But migrating to IP-based solutions, as with any systems, increases the security risk unless robust processes and protections are in place and constantly maintained. The PCI DSS provide clearly defined requirements which, if followed, will prevent the theft of card data.

Why PCI DSS is critical

PCI DSS compliance needs to be at the heart of any card-present transaction system today. Since they were first established in 2004, the guidelines have evolved considerably to accommodate new technologies.

For many organisations, maintaining these regulations is a complex and ongoing process that's time-consuming, expensive and can even limit business agility. But the alternative is far worse, as the impact of a breach can be potentially devasting.

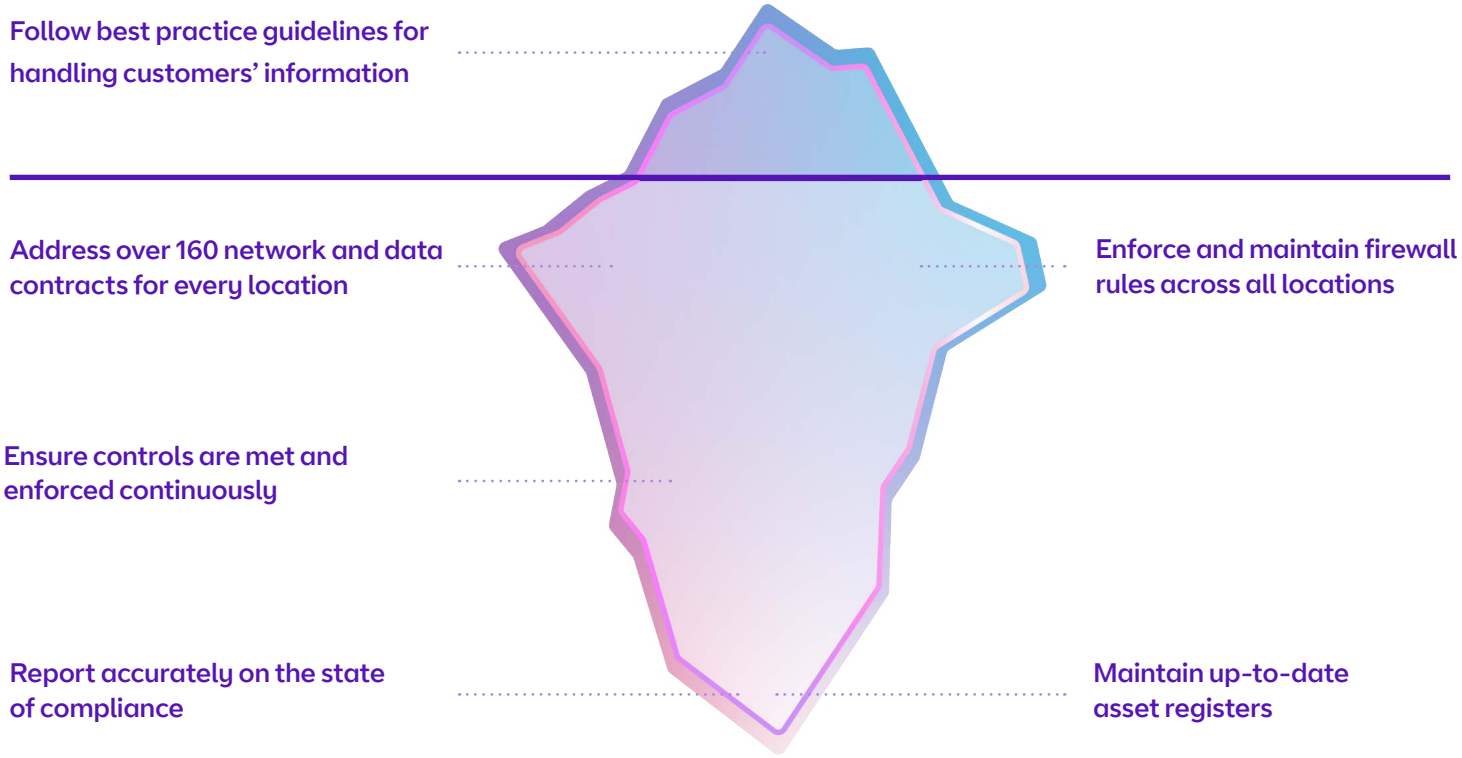
The impact of a data breach violation

In 2021, the average cost of a data breach for a business with under 500 employees was $2.98 million, 38% of which was due to loss of business. According to the same report from IBM, this loss usually extends over several years with around 53% in the first year, 31% in the second, and another 16% of cost still in effect after two years.

Any publicly known breach risks serious damage to your reputation, credibility and customer loyalty and can even result in additional legal issues – plus, for any major global brand it would almost certainly mean long-lasting brand equity damage.

Navigating the compliance challenge

Compliance is critical, and achieving it is complex – especially when many aspects are technologically demanding and challenging to implement and enforce. A good analogy is an iceberg: the most significant risks and challenges aren't the ones that are visible, above the waterline, they're hidden below.



Understanding the iceberg

Above the waterline
These are the physical controls or manual 'best practices' that a merchant's staff are taught to follow when handling information – for example, not storing or noting down card data. Although these procedures are essential, they are just the 'tip of the iceberg' for maintaining card transaction security and compliance.

Below the waterline
These controls concern the POS systems that receive, manage and route payments and the networks they reside in and transmit across. Most PCI DSS recommendations focus on these functions – looking at how merchants secure their payment networks and adequately protect their Card Data Environment (CDE) as transactions are routed to the payment host.

There are over 160 network and data controls for every location, including guidance on appropriate network segregation, securing VPN tunnels and device access rights. On top of this, organisations are expected to continuously monitor any controls and implement updates in accordance with guidance. They are then subject to a robust PCI DSS annual audit to prove their measures are adequate.

The reality of PCI DSS compliance

PCI DSS compliance can look very different depending on the size and type of organisation that's trying to implement it.

Compliance challenges for large, distributed enterprises

For larger, more distributed enterprises, some of the major hurdles to staying PCI DSS compliant are:

- providing an 'always on' resilient network service for critical payment, POS, monitoring and back-office systems
- enforcing and maintaining compliance across thousands of corporately owned and franchised locations and distributed endpoints
- segregating brand and franchisee networks on shared connectivity and infrastructure
- maintaining adequate and accurate reporting on the state of compliance
- securing and segregating network segments at the store such as CDE, Basic Operating Systems, corporate and guest wi-fi networks.

To deal with PCI DSS requirements at scale, most large enterprises will typically employ a Qualified Security Assessor (QSA), approved by the Payment Card Industry Security Standards Council (PCI SSC). A QSA is an independent individual or team tasked with assessing all aspects of the organisation's network across which credit card data flows or resides. Their job is to ensure security is present at every point and that the necessary processes are in place to keep it secure until the next audit.

Compliance challenges for smaller merchants

Smaller merchants face their own challenges in trying to adopt a DIY approach to PCI DSS compliance:

- they often find themselves taking on responsibility for understanding how to secure their network alone
- they're typically self-assessed, often resulting in a self-accredited 'tick-box' approach, that doesn't guarantee their environment is secure or meets security standards
- without the same budgets as larger organisations, sourcing an external compliance consultant is usually far too expensive.

Easily overwhelmed and with far fewer resources to support themselves, many small businesses default to relying on their limited in-house knowledge or just hope for the best. In many cases, they'll complete their Self-Assessment Questionnaire (SAQ) stating they're compliant without any clear understanding of whether they are or not. By doing this, they avoid monthly non-compliance fees but expose themselves to real risks that, in the event of a data breach, will result in considerable fines and a remediation process that can severely impact a business.

What to look for in a card payment solution

Organisations know they need to evolve their payment strategy but are concerned about how to do it without making their lives more complicated and opening the door to regulation and compliance headaches. Achieving a low risk, simple migration to new payment technologies needs to take these factors into account:

- **A wide range of IP-based connectivity options**
  A solution that works with internet, 4G / 5G and MPLS
- **A seamless migration from legacy technology to IP-based payment delivery**
  Allows the transition towards faster, feature-rich IP transactions
- **Full compliance to PCI-DSS standards**
  Removing the burden of ensuring PCI compliance when transmitting payment transactions
- **Supports a wide range of transactions**
  Linking different types of card terminals to merchant acquiring banks and payment processors
- **Supports a wide range of acquirers and processors**
  The flexibility to choose a combination of acquirers and processors, with simple means to switch between them
- **Easy scalability and flexibility**
  Seamless expansion globally using a standardised footprint to transport billions of transactions each year
- **Business continuity and resilience**
  Ability to keep taking payments in the event of network disruption
- **Security built in**
  A solution which incorporates the latest security trends like SASE to prevent tampering at the network edge
- **Around-the-clock support**
  An actively monitored network managed by a dedicated payments specialist helpdesk, 24x7x365
- **Tried and tested reliability**
  A solution that's used and trusted by major banks, payment processors and retailers
- **Future-proofed against future iterations of PCI DSS**
  Technology should be created with the flexibility to adapt to meet new standards

Introducing BT Cardway, with Mako technology

We've reimagined BT Cardway, partnering with managed network security vendor, Mako Networks, to create an 'in a box' payment solution that solves today's problems of security, network and PCI DSS compliance – and is future-proofed for the compliance developments to come. Used and trusted by some of the world's largest retail enterprises, it's a simple route to enhanced security, control, reliability and compliance, and comes with excellent support. It's ideal for both attended and unattended locations.

It comes with flexible deployment options that protect the cardholder data environment without modifying the existing network environment; use it across your whole network, or just deploy it as a zone router to protect your POS environment. Plus, BT Cardway includes retail-specific SD-WAN technology that delivers cost-effective WAN resiliency and redundancy.

BT Cardway with Mako technology is ground-breaking, delivering the world's first PCI-certified networking payment solution.

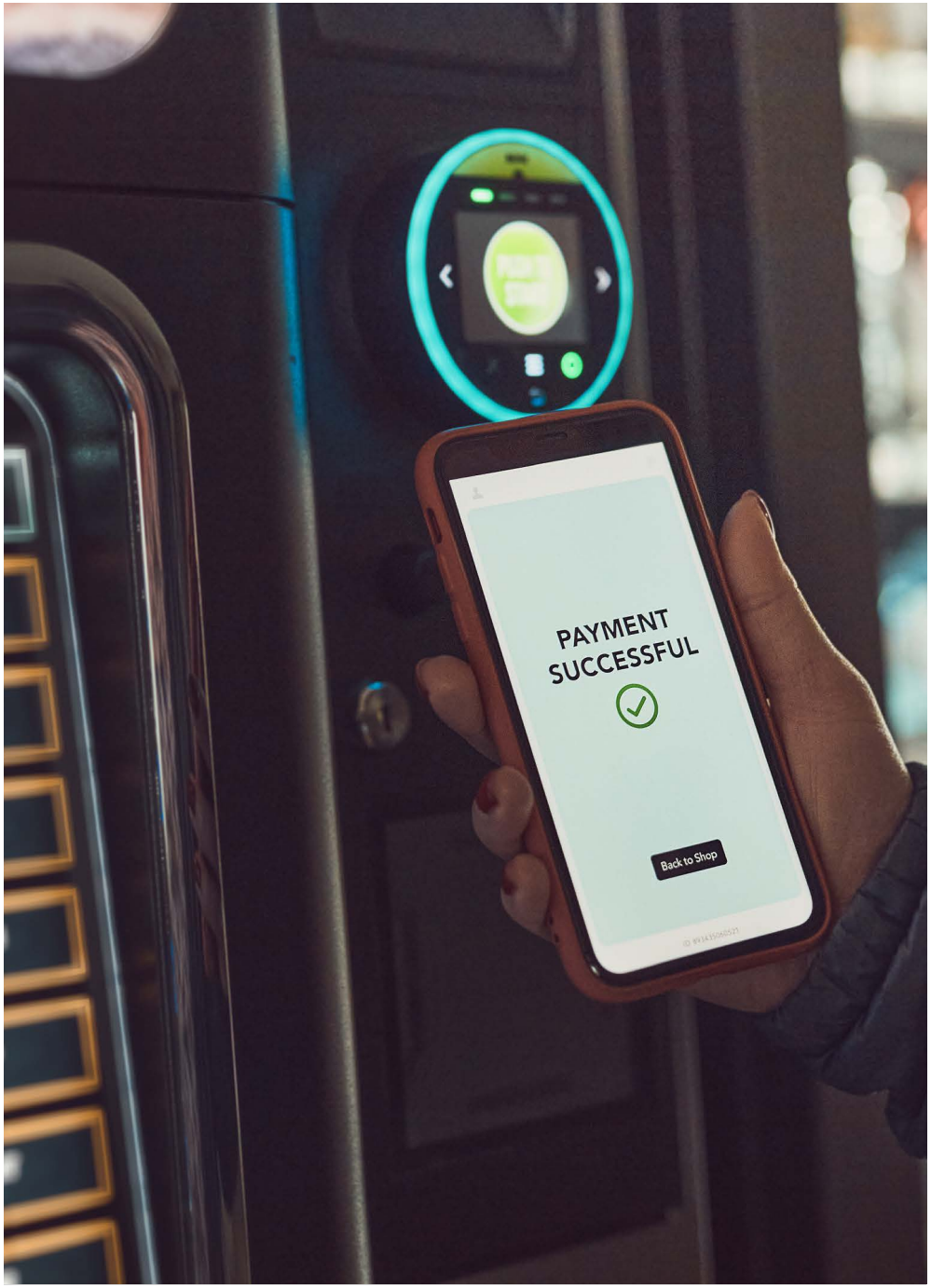
What makes Mako technology unique?

The whole system is PCI DSS Certified
All components of the solution have passed an extremely demanding annual security audit process, which removes retailers' worries about the security and compliance of their payment processes.

The ability to carry out internal vulnerability scans
This removes the need for any additional hardware at site, reducing the cost and complexity of adding and maintaining additional equipment at scale. What's more, when the scans are carried out, Mako's patented VPN Cloud technology initiates automated and secure temporary tunnels which are immediately taken down once the process is complete.

Enterprise template configurations
Using centralised common policies such as firewall rules that integrate with Mako's Merchant PCI functionality, customers only need to review their centralised templated configurations, rather than go out and inspect hundreds or thousands of individual sites.

Mako's Central Management System (CMS)
Mako's system is designed to strictly enforce controls, actively monitor and report on payment networks at a site level to ensure compliance. If any changes are found that'll compromise PCI configuration, it highlights the specific sites that require review. This delivers huge time savings and cuts the risk of sites falling out of compliance without the organisation's knowledge, unknowingly compromising their security posture.



Futureproofing for PCI DSS 4.0

The latest round of PCI DSS will come into full effect from March 2025 onwards. PCI DSS v4.0 centres around 12 requirements that are intended to address emerging threats and market changes. It also takes into consideration flexibility around implementation, the need for stronger security standards and highlights the importance of a continuous self-auditing process to ensure thorough compliance.

How does BT Cardway with Mako technology prepare for this?

Although BT Cardway with Mako technology currently focuses on the compliance challenges of PCI DSS v3.2.1, we designed our solution with v4.0 in mind.

Under PCI DSS v4.0, password and multi-factor authentication requirements will get stricter. But this needn't worry our customers, because the Mako CMS can tune to any PCI version. This means it can easily accommodate these changes, making sure that the transition to v4.0 is straightforward and secure.

Our automated internal scans will also remain PCI DSS certified, meaning there's no need for customers to carry out their own internal scans. Plus, our upcoming Mako Merchant PCI service, due to be released in the first quarter of 2023, will deliver a brand-new estate-wide compliance dashboard to provide clear visibility for merchants across their multiple sites and franchises.

A complete solution

BT Cardway with Mako technology is a resilient, secure payment networking solution for new or existing customers. It handles everything to do with card-present payment transactions and makes enforcing and maintaining PCI DSS network compliance easy, no matter the size of your merchant's estate. This way, you can get the most from IP technology, knowing your transactions are protected all the way from the point of sale to the payment host.

It's largely automated and simple to deploy, manage and maintain, so you won't need to do any additional or bespoke engineering. We've also included back-up features to ensure BT Cardway can operate almost entirely independently in the event of a network failure.

BT Cardway with Mako technology features:

Cellular failover
With fast LTE or 5G cellular backup connection, our cellular failover ensures payments keep on flowing if the primary broadband service is disrupted.

Cloud-based management
With our role-aware, cloud-based CMS, technical support staff can achieve complete network configuration and visibility and managerial staff can see and understand what's happening in their network. Plus, for any additional queries technical support is available over the phone 24 / 7.

Status alerts
Organisations receive real-time and proactive email notifications of potential network concerns and important events such as malware threats and internet connectivity issues.

Virtual Private Networks
Our solution delivers secure, encrypted connections between your retail locations and your main office or data centre to share information.

Content filtering
Control internet usage by blocking sites that may be inappropriate or taking up bandwidth at your business.

Usage reporting
Get detailed reports on internet usage to help you monitor how your staff and guests are using the internet.

Built-in wi-fi
The Mako edge devices include built-in wi-fi, and additional access points are available should you need to cover larger environments.

BT Cardway in action

Delivering resilience and compliance to the energy sector

The challenge
A major petroleum brand, with corporate and franchise sites, needed to modernise its WAN / retail LAN infrastructure to improve resilience and payment security compliance across their estate. They also wanted to allow their franchisees to use the same solution for their own, non-POS purposes.

The solution
We deployed and managed Mako devices across all sites using templated configurations. These included Mako VPN Cloud tunnels to ensure all their data is secured in transit, PCI templates to secure their CDE and Enterprise templates to enforce a PCI DSS compliant firewall and VPN rules for both their brand and franchise locations. Franchises were then given control over non-CDE network segments. Finally, to increase resilience, we included high availability failover options.

The result
The brand can now centrally manage their critical controls across every site and ensure they can't be altered, while their franchises retain independent control over their individual back-office or configuration preferences. They're now always PCI compliant and when it comes to annual audits, reporting is hugely simplified. Plus, with their new high-availability failover options, they know that data and transactions will remain uninterrupted in the event of a failure.

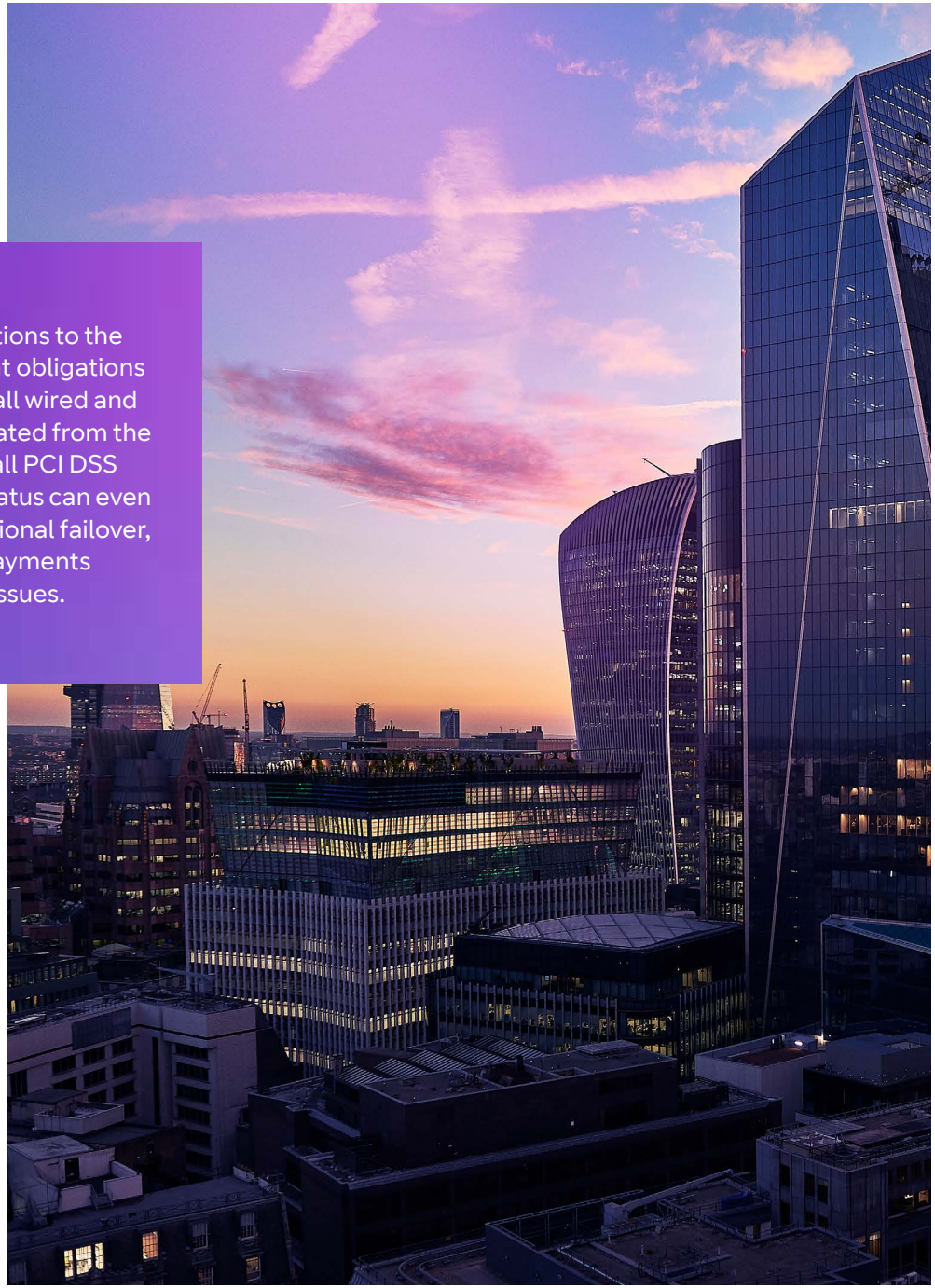
BT Cardway in action

Simplifying compliance in the financial sector

The challenge
An acquiring bank with thousands of Level 4 merchants that were struggling to achieve PCI DSS compliance. The acquiring bank was concerned that some merchants might be relying on a ‘tick box’ self-assessment approach that risked not having the appropriate controls in place.

The solution
We deployed Mako devices as secure payment zone routers with optional failover. Then, we further protected their transaction traffic with Mako VPN Cloud tunnels to the payment host.

The result
Now, all merchants meet their obligations to the bank and the bank meets all merchant obligations to the card schemes. This is because all wired and wireless POS devices are now segregated from the rest of the merchants’ networks and all PCI DSS controls are enforced. Compliance status can even be reported in real time. With the optional failover, they are also guaranteed non-stop payments regardless of any upstream network issues.



Compliant payments made simple

BT Cardway with Mako technology is a simple way to navigate through a sea of compliance complexity. In one product you get a carrier-grade-compliant, resilient payment system that's ready to support your organisation today – and into the future.

To find out more about how BT Cardway can support your payments, get in touch with your account manager.

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

January 2023