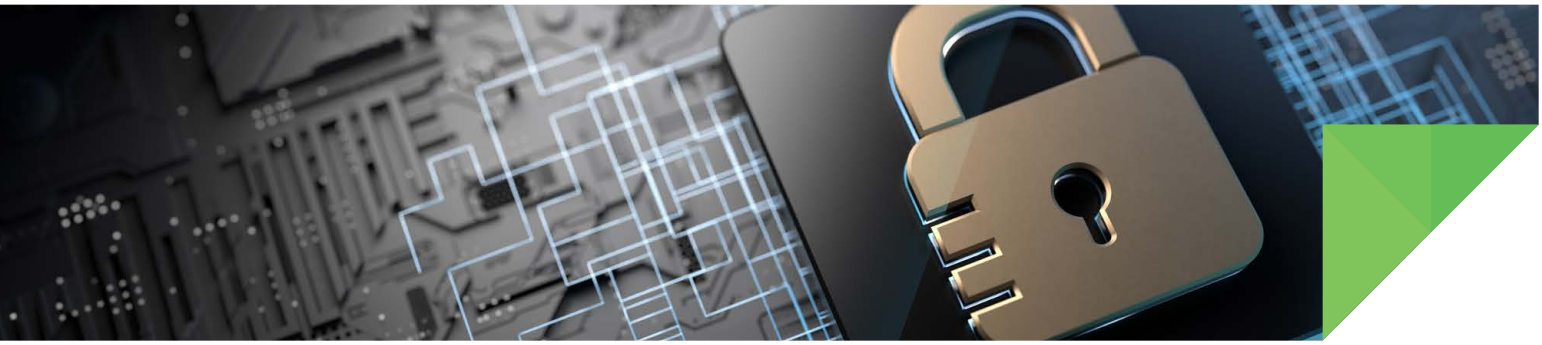
PCI-COMPLIANT CELLULAR CONNECTIVITY WITH DIGI ENTERPRISE ROUTERS



Introduction

This white paper explains the purpose and key concepts involved in PCI compliance and describes the elements of a payment network. Additionally, it illustrates how Digi enterprise routers and cellular extenders help merchants and managed service providers serve their customers while maintaining PCI compliance. After reading this document, a network engineer or network administrator will understand the PCI-relevant features and configuration elements of Digi cellular routers.

Key concepts include:

Overview of PCI, including business drivers, terms, roles, and documentation, as well as specific Digi router configurations to support PCI compliance:

- Enabling stateful packet inspection (SPI) firewall on WAN interfaces
- Use of encryption and authentication via IPsec VPN, SSL, SSH, SFTP and/or X.509 certificates
- Segmenting the network via VLAN or Ethernet port isolation, as needed
- Configuring user accounts, admin levels and remote authentication (RADIUS/TACACS+)
- Monitoring and managing the router via SNMP v3 and/or **Digi Remote Manager®**
- Storing log events with Syslog, including event alarm support via SNMP, email and/or SMS
- Using Digi Remote Manager for device profiling and firmware management

Next, we will discuss how you can evaluate the best way to optimize your IP and make the right build-vs.-buy decision to meet your goals.

Why PCI Compliance Matters

It seems like every week we have new stories about high-profile data breaches in the retail industry. The unsurprising result is that consumers are more concerned about data security and privacy than ever before and are demanding stronger security. Therefore, merchants and the managed service providers (MSPs) who support them are eager to maintain customer goodwill, prevent lawsuits, avoid fines, and stay out of the media.

Merchants who accept credit and debit cards using a financial institution's payment networks must comply with the Payment Card Industry (PCI) Data Security Standards (DSS). Digi International, an industry leader in machine-to-machine (M2M and IoT) connectivity solutions, integrates security into every aspect of its product-development lifecycle. Digi cellular routers meet the strict security requirements of PCI DSS. They can be deployed as part of a cardholder data environment (CDE) to meet all PCI-DSS requirements with minimal overhead and management.

An Overview of PCI DSS

From Point-of-Sale (POS) merchants to banks, the entire retail/financial continuum is charged with implementing a PCI-compliant infrastructure to handle credit/debit-card transactions. The PCI Security Standards organization maintains a library of documentation that helps to define and clarify these requirements.

In the pages that follow, we will discuss each of the 12 key PCI-DSS requirements and explain how a Digi cellular router can be a key component of a PCI-compliant system. Please note that these requirements are subject to interpretation. A qualified security assessor (QSA), approved scanning vendor (ASV), or auditor may interpret the rules differently, find vulnerabilities, or make recommendations that exceed or vary from PCI DSS requirements. Digi routers can nearly always be configured to comply with these different interpretations.

It's important to remember that, except for PIN entry devices (PEDs), there are no specific PCI device certifications. By definition, no network device, such as a Digi router, can be accurately called "PCI certified." However, these devices can be secured and managed in a manner that achieves and preserves PCI-compliant security. Security standards such as NIST and FIPS may be also recommended by a QSA or ASV. PCI does not require, for example, FIPS-140, ICSA, or other device certifications.

Let's begin by understanding the different roles and acronyms used by payment network operators and vendors in the industry.

1. **PCI SSC** (Payment Card Industry Security Standards Council): This global forum was founded by five global payment brands (American Express, Discover, JCB, MasterCard and Visa) to develop and manage security standards, including PCI DSS. Digi is a participating member of the PCI SSC.
2. **PCI DSS** (Payment Card Industry Data Security Standard): This is what most people mean when they refer to "PCI." This standard defines 11 baseline technical and operational requirements that service providers must meet.
3. **PA-DSS** (Payment Application Data Security Standard): This standard is specifically designed to help software vendors develop secure payment applications.
4. **PTS** (PIN Transaction Security): This is a security program for manufacturers who build PIN entry devices (PEDs).
5. **QSAs, ASVs, and SAQs** (qualified security assessors, approved scanning vendors, self-assessment questionnaires): Professionals and methods for validating PCI DSS compliance.
6. **ROCs and AOCs** (reports on compliance and attestations of compliance): PCI compliance validation documents.

Every merchant, processor, and service provider who uses the global payment network must adhere to the PCI DSS framework. Regardless of which compliance validation paths you choose — QSA, ASV, or SAQ — the 12 requirements on page 5 must be met.

Goal	Requirement
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures	7. Restrict access to cardholder data by "need-to-know" basis. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel.

The Security of Digi Cellular Routers

For over three decades, Digi has been a leading supplier of communications solutions for retail/POS, kiosk, banking and ATM markets. Digi routers provide secure high-speed wireless connectivity to remote sites and devices. These routers can be used for primary wireless broadband network connectivity or backup to existing landline communications.

Digi routers are differentiated through their advanced routing, firewall and security features, including stateful packet inspection firewall and integrated VPN. Enterprise class protocols incorporate BGP, OSPF and VRRP+, a patented technology built upon the popular VRRP failover standard providing auto-sensing, auto-failover, and auto-recovery of any routing failures.

Digi enterprise products meet PCI security requirements while providing secure credit card data processing and transmission. Through a range of security features, Digi solutions simplify PCI compliance. These security features include:

1. **Security testing:** Digi devices undergo complete testing using several tools and techniques. These tools include common vulnerability scanners such as Rapid 7's Nexpose, Nessus, and the BuRP application testing suite. Additionally, Digi engineers use a technique called "fuzzing" to find security vulnerabilities within devices and code.

What is "Fuzzing"?

Originally developed by Barton Miller at the University of Wisconsin in 1989, fuzz testing or "fuzzing" is a software testing technique to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, or "fuzz," in an attempt to make it crash. If a vulnerability is found, a tool called a fuzz tester (or fuzzer), indicates potential causes. Fuzz testing is simple and offers a high benefit-to-cost ratio. Fuzz testing reveals defects that are overlooked when software is written and debugged.

Source: Tech Target: http://searchsecurity.techtarget.com/definition/fuzz-testing

2. **External pen testing:** Digi cellular routers have successfully passed external hardware and software reviews by world-class companies and universities, including penetration testing (or "pentesting"). These evaluations focus on protecting the confidentiality and integrity of data flowing through the device and validate the internal coding of its security algorithms. This includes the algorithm of the AES encryption standard, the cryptographically secure random number generator, and all hash functions. The evaluations found that the Digi devices meet or exceed public security standards. Working with partners at customer sites, universities, and security firms, Digi evaluates and responds to new threats, aiming to make Digi routers the world's most secure. Visit our **security page** for additional information.

What is "Pen Testing"?

Penetration testing is the attempt to gain access to resources without knowledge of usernames, passwords and other conventional access credentials. What separates a penetration tester from an attacker is that the penetration tester has permission from the resource owner and is responsible for reporting the findings. In many cases, a penetration tester has user-level access and seeks to elevate the status of the account or use other means to gain access to additional information that a user of that level should not be able to access.

Source: SANS Institute: https://www.sans.org/reading-room/whitepapers/analyst/penetrationtesting-assessing-security-attackers-34635

3. **Documentation:** Find your product on Digi.com to access the available resources, or search for your product's user guide at **www.digi.com/documentation**.

4. **Private cloud infrastructure:** While there are concerns that some cloud services are not as secure as private data centers, the cloud can provide better security than a traditional data center when implemented correctly. Digi isolates and hosts its own private cloud environment. This means that applications are not shared with other cloud customers, so security can be applied properly without sacrificing reliability or scalability.

5. **World-class data center:** Digi Remote Manager is housed in one of North America's most secure data centers, operated by one of the world's best trained teams of experts.

6. **PCI DSS scope:** PCI compliance is a challenging task. The first step is to understand the scope, which can encompass any item that transmits, processes, or stores credit card information or is directly connected to the cardholder environment (also called the "cardholder data environment" or CDE). The scope of PCI also includes any system that can directly affect the security of the CDE. If you have a vendor who is providing configuration or other security services through an application to your devices, the application and all of its supporting components are in scope for PCI DSS. Many vendors claim the security services they provide for devices are not under scope or are not under scope because of a private APN. This is not the case.

For more information, consult the PCI Council statement on **third-party security assurance**.

Digi Cellular Router Features That Enable PCI-Compliance

Requirements	Digi Cellular Router Features
1 Install and maintain a firewall configuration to protect cardholder data	Digi has sold over half a million highly secure, long-life cellular routers in 95 countries and is a key provider of network migration services as businesses move to faster, more reliable technology.
2 Do not use vendor-supplied defaults for system passwords and other parameters	Digi helps the network administrator by supporting user authentication tools such as RADIUS and TACACS+.
3 Protect stored cardholder data	Not applicable — no cardholder data is stored.
4 Encrypt transmission of cardholder data across open, public networks	Digi uses IPSec and SSL authentication and 3DES and AES 256-bit encryption, as well as X.509 certificates and SCEP for authentication. Digi also supports private-network options from multiple cellular carriers.
5 Protect all systems against malware and regularly update antivirus software or programs	Digi regularly releases firmware with feature enhancements and fixes to any known security issues. This firmware is available for free on **www.digi.com** and can be delivered remotely using Digi Remote Manager.
6 Develop and maintain secure systems and applications	Digi assists network administrators with Digi Remote Manager, which auto-scans devices and forces compliance to a "golden" configuration to thwart tampering.
7 Restrict access to cardholder data to those with "need to know" basis	Digi provides TACACS+, RADIUS, and event logging via syslog.
8 Identify and authenticate access to system components	Digi provides TACACS+ and RADIUS support. Administrators can store multiple user logins, each with different authority levels (including read-only).
9 Restrict physical access to cardholder data	Digi cellular routers can use multiple mounting options and external antenna options, as well as SIM door covers for additional security. Serial, USB, and Ethernet ports can all be disabled for additional physical security.

10	**Track and monitor all access to network resources and cardholder data**	Digi cellular routers offer configurable event logs with syslog support and time synchronization via NTP or SNTP.
11	**Regularly test security systems and processes**	Event and firewall logs help diagnose network issues. Digi Remote Manager detects changes in device configuration and network performance, including packet loss, latency, signal strength, data usage and other metrics.
12	**Maintain an information security policy for all personnel**	Digi supports network administrators through simple text-based configuration files and event logs, and provides advanced alarms and reporting through SNMP-based tools and Digi Remote Manager.

A Closer Look at How Digi Cellular Routers Enable Strong PCI Compliance

Install and maintain a firewall configuration to protect cardholder data. Digi routers include an exceptionally powerful and flexible stateful inspection firewall. Most devices in this category have simple on/off options for their firewalls. By contrast, Digi cellular routers support full scripting and can be tailored to suit most firewall implementations. Dynamic filters are more secure because session information is constantly monitored to track and match requests and replies. In addition, the firewall automatically verifies that the correct flags are used for each stage of communication.

Requirement 1 calls for more than simply providing a firewall. Network Address Translation is also part of this requirement. Digi cellular routers provide RFC 1918 NAT and NAPT on any interface to hide "private" IP addresses from the Internet and translate those addresses into the public address of a "public" WAN. By its very nature, NAT blocks any unsolicited traffic not destined for the router itself. Enterprise routers have a simple option to disallow any "external" remote management on an interface.

Several subsections of Requirement 1 define DMZ support. For instance, Requirement 1.1.3 states that a firewall must be installed at each Internet connection and between any DMZ and the internal network zone. Digi provides several mechanisms to segregate DMZ traffic.

A Digi router's stateful firewall can block, pass and redirect traffic based on IP address and/or service port using firewall rules and/or NAT port forwarding. Static NAT mapping is also possible: redirection can also be used for WAN failover where firewall rules test the health of the primary WAN connection and redirect that traffic through another interface.

The built-in four-port Ethernet switch on certain Digi models provides easy segmentation for up to four distinct and separate networks — each with its own DHCP server, if desired. This is called port isolation mode. One or more of these networks can be designated as a DMZ, allowing Digi routers and firewalls to segregate traffic as required. For example, you could put POS devices on a network that is separate from the back-office system.

VLAN tagging is supported for network segmentation when only one IP subnet is used (e.g., the "store" has one IP network using 192.168.1.0/24 and Ethernet port isolation is not used) or only one Ethernet port is available. VLAN tagging prevents traffic from one VLAN from being visible on another VLAN.

Requirement 1 also calls for secure and synchronized router configuration files. Digi Remote Manager can store and compare configuration files. Some third-party applications can also analyze and compare Digi router text-based configuration files. The Event Log can send an alert if changes are made or when someone logs into the router.

Perimeter firewalls can be installed between wireless networks and the CDE to control any traffic from the wireless environment.

Do not use vendor-supplied defaults for system passwords and other security parameters. For older Digi router models, a network administrator must properly secure the device by changing appropriate settings, particularly the default username and password. Newer Digi routers all ship with unique credentials. Digi routers provide complete control over these settings. Multiple users can be configured on the device with various access levels and can optionally be authenticated via RADIUS or TACACS+.

Protect stored cardholder data. Digi routers do not store cardholder data. They do feature something call the "Analyzer," a powerful layer one and two protocol diagnostic tool that allows frames to be analyzed via text or Wireshark capture files.

This feature can be configured so that the Analyzer trace stores only partial data of every transmission, allowing some limited diagnostics without storing sensitive cardholder data. The Analyzer can be disabled altogether or limited to certain interfaces and protocol layers.

Requirement 3 also addresses cryptographic keys. Digi routers support X.509 certificates including SCEP support. IKE key management for IPsec is also available via pre-shared keys or certificates. These mechanisms ensure proper authentication and secure transmission of card data.

IPsec and SSL are provided on Digi enterprise routers to protect and authenticate data transmission. 3DES and 256-bit AES encryption and SHA-1 authentication hash algorithms are supported. As mentioned, X.509 digital certificates and SCEP enrollment are supported for authentication.

Encrypt transmission of cardholder data across public networks. Requirement 4 concerns traffic across a public network. Wireless WANs work much like DSL, cable modems or other wired broadband connections. Work with your carrier to implement a plan that meets your security needs and budget. The following are three carrier-related options that can help secure traffic across a wireless WAN:

1. **Block traffic from the mobile network.** Many carriers have plans that only permit remote-initiated traffic. Firewalls inside the carrier network block any unsolicited inbound traffic. However, this plan cannot be used if your application requires you to reach out to remote sites to poll a bill pay terminal (some carriers call this mobile-terminated data), unless IPsec VPN is used from the mobile device. Other carrier plans may block only some traffic such as HTTP on port 80 or pings, or they may use restricted IP addresses that use public IP addresses but access is restricted internally by the carrier.

2. **Use a completely private plan.** Here, the carrier supplies a direct connection into your network via private circuit, usually by Frame Relay, MPLS, or IPsec VPN, which is known only to you. This means that devices not owned by you cannot attach to your private part of the cellular network. In many cases, private IP addresses can be assigned to the Digi router's mobile interface and controlled by you. The data never touches the Internet.

3. **Use dynamic mobile IP addresses but do not use Dynamic DNS.** While this is an available option, it will likely restrict your application to only outbound initiated connections.

A side benefit of the first two options above is that these plans also block unwanted billable traffic to save you money. Any connection attempt that traverses the wireless carrier network to the mobile IP address can be viewed as billable traffic, even if the mobile device blocks the connection attempt.

Protect all systems against malware and regularly update antivirus software or programs. Digi regularly releases new firmware to improve features, fix bugs, and patch new security risks. However, unlike other enterprise router vendors who charge for firmware updates or enterprise software licensing, Digi provides the latest firmware for free and offers turnkey delivery of firmware through Digi Remote Manager — regardless of network size.

Develop and maintain secure systems and applications. Requirement 6 is primarily aimed at users who maintain and test applications and systems. Digi strives to update device operating firmware in accordance with customer needs. Firmware updates are available via the Digi support site and are free of charge.

Easily activate, monitor and diagnose hundreds or even thousands of mission-critical devices from a single point of command with Digi Remote Manager.

Digi Remote Manager can regularly scan the state of devices and identify any deviations from a “golden” configuration. This will reset the configuration and bring attention to any attempted configuration changes or hacking. For example, Digi Remote Manager can identify if an unauthorized user has created a backdoor password and will return the configuration to its approved parameters and send an alert. The Event Log can also issue alarms if any changes are made to a device.

Restrict access to cardholder data by need-to-know basis. User authentication can be accomplished via TACACS+ or RADIUS. Only currently authorized logins are allowed to access the device and all access is logged in the Event Log.

User access to cardholder data can also be partially controlled by MAC filtering, VPN, and firewall policies. For example, a VPN policy could limit which client IP addresses can access the remote network. MAC filtering can prevent an unauthorized laptop from gaining access to the Digi router.

Identify and authenticate access to system components. As with Requirement 7, TACACS+/RADIUS authentication prevents unauthorized access. In addition, Digi router can store multiple user logins, each with an assigned authority level. In particular, only users with "Super" access can create logins for other users. Read-only users can also be created.

Restrict physical access to cardholder data. This requirement depends heavily on sensible placement of devices. For example, it would be unacceptable to locate Digi routers behind store counters where staff and consumers could easily have access.

The first instinct is to simply lock the Digi router in a wiring closet or back office. That provides strong physical security — but that may not be an optimal location if it impedes access to the cellular data network. All Digi routers can use remote antennas so that the router remains stored safety while still enjoying optimum signal quality.

Keep a list (and store it separately) of all MAC and IP addresses, ESNs/IMEIs, SIM IDs, and associated phone numbers so that devices can be disabled by the carrier in the event of theft.

Antenna security is also important. Mount external antennas securely to prevent theft and weather damage. Unobtrusive, low-profile antennas are available from various sources.

If the router is in a visible location, physical access to the router can be minimized. First, the console port(s) can be disabled to prevent unauthorized local access. Firewall or MAC filtering can make any unused Ethernet ports inaccessible except for allowed traffic. USB ports can be disabled (note there is no user "login" access to Digi devices via USB; USB ports are solely for devices such as GPS receivers and expanded memory). Companies such as Panduit manufacture RJ-45 hardware locks that cover open jacks and can only be removed with special tools. Additionally, each power-up can be reported via syslog to a central server so that the reason for the disconnection can be investigated.

Track and monitor all access to network resources and cardholder data. The Digi router event log tracks access and changes to the device. The event log can be saved to syslog. The event log is fully configurable so that some events can be logged while others are omitted. For example, logging of user access and changes is needed, but ADSL or cellular events are not. Events can also be configured to raise alarms via the event handler. Alarms can be sent via email, SNMP and (on certain models) SMS text messages. Time synchronization can be done via NTP or SNTP on the Digi router, and (in some cases) via the cellular network itself.

Regularly test security systems and processes. Testing systems and processes are up to the user, auditor, or approved scanning vendor (ASV). Digi Remote Manager detects changes in device configurations and network performance, including packet loss, latency, signal strength, data usage and other metrics. The Digi router event and firewall logs and Analyzer can also help track and diagnose network traffic issues.

You can verify configuration file integrity using any number of tools. The Digi router configuration files are flat text files that are readable by many compliance tools. Digi Remote Manager can also detect changes in standard configurations.

If the router is on the Internet (see above about using private data plans), it will likely be subjected to connection attempts on a daily basis by automated hacker scripts — just like any other Internet-

connected router. Many of these tools attempt to take advantage of known security problems with operating systems, applications, and even routers. They also attempt to connect using default usernames and passwords, etc.

Detecting these attacks on Digi routers itself can be done using several mechanisms, such as alarming via the event and firewall logs. However, the key is to prevent the attack by properly configuring a Digi router's firewall rules and enabling the “block remote access” option on WAN interfaces.

Maintain a policy that addresses information security for all personnel. It’s the user’s responsibility to create and maintain effective security policies. The Digi router's simple text-based configuration files and event logs make it easy to view and confirm they adhere to the policies. Digi Remote Manager is also an effective tool for notifications of real-time security threats. Digi router event alarms and Digi Remote Manager can alert personnel of any problems or changes to configurations.

Conclusion

More than ever before, consumers, retailers, and financial institutions are focusing on the critical importance of security in the card payment cycle. In this environment, airtight PCI compliance has become a “must,” leading many stakeholders and participants to seek guidance and support. Digi solutions help enterprises achieve PCI compliance.

Key Takeaways:

- ✔ Merchants who accept credit and debit cards using a financial institution’s payment networks must comply with the Payment Card Industry (PCI) Data Security Standards (DSS).
- ✔ To achieve PCI compliance, meet 12 PCI requirements that cover infrastructure, communications and policy.
- ✔ Digi products offer enterprise-class features that meet rigorous PCI-DSS security requirements.

Digi's enterprise routers offer the industry’s strongest support for PCI-DSS compliance, addressing every relevant requirement of the rigorous standard. Learn more about Digi cellular routers **here.**

Why Digi?

Digi is a complete IoT solutions provider, supporting every aspect of your project, from mission-critical communications equipment to professional services to get your application designed, installed, tested and functioning securely, reliably and at peak performance.

Digi builds its products for high reliability, high performance, and versatility so customers can expect extended service life, quickly adapt to evolving system requirements and adopt future technologies as they emerge. Digi cellular routers, servers, adapters and gateways support the latest applications in traffic, transit, energy and smart cities.

Our solutions enable connectivity to standards-based and proprietary equipment, devices and sensors, and ensure reliable communications over virtually every form of wireless or wired systems. An integrated remote management platform helps accelerate deployment and provide optimal security using highly efficient network operations for mission critical functions such as mass configuration and firmware updates, including system-wide monitoring with dashboards, alarms and performance metrics.

Company Background

- Digi is publicly traded on the NASDAQ stock exchange, symbol DGII
- Founded in 1985, Digi has 35+ years of experience connecting the “things” in the “Internet of Things” — devices, vehicles, equipment and assets
- Headquartered in the Twin Cities of Minnesota, Digi employs over 550 people worldwide
- The business has been profitable for 15 consecutive years
- Digi’s annual revenue is around $250 million
- The company has 285 patents issued and pending (150 issued)
- In our three decades in business, we have connected over 100 million devices

As a communications equipment manufacturer, Digi puts proven technology to work for our customers so they can light up networks and launch new products. Machine connectivity that’s relentlessly reliable, secure, scalable, managed — and always comes through when you need it most. That’s Digi.

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

/digi.international @DigiDotCom /digi-international