Dawgen GLOBAL

2026 EDITION



Dawgen Global illustration

CYBERSECURITY SERIES · TECHNOLOGY & CYBER

Payment & Banking Security

Protect every transaction, from card to core.

PCI DSS readiness, ATM and card security testing, SWIFT security assessments and digital banking security for banks, credit unions, payment providers and merchants.

SECURE THE PAYMENT. MEET THE STANDARD. KEEP CUSTOMERS' TRUST.

01 · THE BUSINESS ISSUE

Payment systems are the prime target.

Banks, credit unions, payment providers and merchants across the Caribbean process card, mobile and wire payments every second. Attackers target each link in the chain, from ATMs and card terminals to payment messaging and online banking.

Card data is valuable

Stolen card data is sold quickly, and breaches lead to card scheme penalties, reissue costs and lost trust.

ATMs and terminals are attacked

Skimming, malware and physical attacks target ATMs and point-of-sale devices.

Payment messaging is targeted

Attacks on interbank payment systems have caused large losses worldwide.

Standards keep rising

PCI DSS version 4.0 and payment network security requirements set higher expectations for controls and testing.

WHERE PAYMENT SECURITY BREAKS DOWN

- Card data stored where it should not be
- Untested ATM and terminal security
- Weak segmentation around payment systems
- Shared administrator accounts on payment servers
- Third-party processors not assessed
- Online banking open to account takeover

> **Payment security protects more than data. It protects the trust that keeps customers using your services.**

02 · OUR SERVICES

Security across the payment chain.

We assess and test every part of the payment chain, and help you meet the standards your card schemes, regulators and partners require.

PCI DSS readiness

Preparing for compliance.

- Scope reduction and data discovery
- Gap assessment against PCI DSS v4.0
- Remediation support

ATM & terminal testing

Testing the machines.

- ATM security assessments
- Point-of-sale terminal testing
- Kiosk and self-service devices

Payment messaging security

Protecting interbank payments.

- SWIFT customer security assessment support
- Payment system segmentation review
- Operator access controls

Digital banking security

Online and mobile channels.

- Online banking testing
- Mobile wallet and app testing
- Account takeover and fraud scenarios

Payment partner risk

Assessing who you rely on.

- Processor and acquirer reviews
- Card issuing partner assessments
- Contractual security requirements

WHO WE SERVE

Commercial banks · credit unions · payment service providers · card issuers and acquirers · remittance companies · merchants and hotel groups accepting cards · fintech wallets.

PCI DSS validation reports are issued by a Qualified Security Assessor where required. We support readiness and remediation.

03 · OUR APPROACH

Scope, test, fix, maintain.

Our payment security work begins by understanding how payments flow through your organisation, then tests and strengthens each point where they could be attacked.

01

Map the flows

We trace how card data and payment instructions move through your systems, people and partners.

02

Reduce scope

We help remove card data from places it does not need to be, shrinking the systems in scope.

03

Assess and test

We assess controls against PCI DSS and payment network requirements and test ATMs, terminals and channels.

04

Remediate

We support your teams to close gaps, with clear priorities and evidence.

05

Maintain

Periodic testing and reviews keep you compliant as systems change.

SCOPE FIRST

Reducing where card data lives is often the fastest way to lower cost and risk.

STANDARDS WE WORK WITH

- PCI DSS v4.0
- PCI PIN and terminal guidance
- SWIFT Customer Security Controls Framework
- Central bank technology risk guidance

CERTIFIED TEAM

Our cyber specialists hold recognised certifications such as OSCP, CEH, CISM, CCSP and ECIH.

04 · PCI DSS READINESS

A clear path to PCI DSS compliance.

Any organisation that stores, processes or transmits card data must meet PCI DSS. Version 4.0 brings new requirements for authentication, monitoring and risk analysis.

Discover

Find where card data is stored and flows.

Assess

Measure controls against each requirement.

Remediate

Close gaps and gather evidence.

A TYPICAL READINESS PROJECT

01 **Scoping**

Data flows and systems in scope agreed.

02 **Gap assessment**

Controls tested against PCI DSS.

03 **Remediation**

Priority gaps fixed with your teams.

04 **Evidence**

Documentation ready for validation.

KEY PCI DSS V4.0 THEMES

- Multi-factor authentication for access to card data
- Targeted risk analysis
- Stronger logging and monitoring
- Phishing and script attack protection

FOR MERCHANTS TOO

Hotels, retailers and e-commerce businesses accepting cards also need to comply.

05 · ATM, TERMINAL & MESSAGING SECURITY

Testing the machines and messages behind every payment.

ATMs, card terminals and payment messaging systems need specialist testing. We assess them against known attack techniques and industry security requirements.

ATM and terminal testing

Physical and logical attacks.

- Malware and black box attack resistance
- Network and host security
- Physical access to internals
- Card skimming protections

Payment messaging

Interbank and wire payments.

- Segmentation of the payment environment
- Operator and administrator controls
- Transaction monitoring
- Annual security attestation support

LINKED SERVICES

Managed SOC
24/7 monitoring of payment systems.

Red teaming
Goal-based tests targeting payments.

Forensics
Investigation when fraud occurs.

> **Attackers look for the weakest link in the payment chain. Testing every link closes the gaps they rely on.**

06 · WHO SHOULD CONSIDER THIS SERVICE

For everyone who moves or accepts money.

Commercial banks with card, ATM and wire payments

Credit unions issuing cards and running ATMs

Payment service providers processing for merchants

Remittance and wallet providers moving money across borders

Hotels and retailers accepting cards every day

Fintech companies launching payment products

07 · ILLUSTRATION

A credit union prepares for card issuing

Situation. A credit union preparing to issue its own debit cards and expand its ATM network needed to meet PCI DSS and its card scheme's security requirements.

Our work. We mapped card data flows, reduced the systems in scope, completed a PCI DSS gap assessment, tested ATMs and the card management system, and supported remediation.

Outcome. The credit union launched its card programme on schedule, with documented controls ready for validation and a programme of annual ATM testing in place.

Anonymised composite illustration based on regional experience.

WHAT YOU RECEIVE

- Payment data flow map
- PCI DSS gap assessment
- ATM and terminal test reports
- Payment messaging review
- Remediation plan and support
- Evidence pack for validation

08 · ENGAGEMENT OPTIONS

Choose the support you need.

PCI DSS readiness

Scoping, gap assessment and remediation support.

ATM and terminal testing

Specialist device security testing.

Payment messaging review

Interbank payment security assessment support.

Digital banking testing

Online and mobile banking security.

Fees are tailored to each organisation and agreed in the engagement letter once scope and deliverables are confirmed.

WHY DAWGEN GLOBAL

- **Caribbean insight.** Over 24 years serving Caribbean business.
- **One desk, 35 territories.** Centrally managed from our Caribbean headquarters.
- **Certified specialists.** Offensive, defensive and forensic skills in one team.
- **Joined-up advice.** Cyber, audit, risk, legal and data protection together.

09 · START HERE

- Request a payment security proposal
- Book a PCI DSS scoping session
- Ask about ATM and terminal testing

CONTACT

Email
info@dawgen.global

Web
https://www.dawgen.global/

Territory desks
Write to your territory desk at *territory*@dawgen.com (for example guyana@dawgen.com). Jamaica: info@dawgen.global

Headquarters
Dawgen Towers, 47-49 Trinidad Terrace, Kingston 5, Jamaica

AUDIT & ASSURANCE · TAX ADVISORY · TECHNOLOGY & CYBER · FINANCE & BPO · GROWTH & RECOVERY · HR & LEGAL

This brochure provides general information only and is not professional advice. Services are provided only under a signed engagement letter. The illustration is an anonymised composite and does not describe any single client.

Dawgen Global is an independent, integrated multidisciplinary professional services firm and is not a member of any international network. As a multidisciplinary firm, Dawgen Global offers some regulated services; in each case the head of the regulated division holds the appropriate professional practice licence in the respective jurisdiction. Some regulatory services are performed by affiliated firms, and clients are advised of this when a request is made.

BIG FIRM CAPABILITIES. CARIBBEAN UNDERSTANDING. · © 2026 Dawgen Global.