

SESSION 11

E-Commerce Security & Trust

SSL • Cybersecurity • Data Protection • Trust

E-Commerce | Winter 2026 | 3rd Year Bachelor

Session 10: Shopify and Turnkey E-Commerce Solution



Shopify Platform

SaaS e-commerce platform — 4.6M+ stores, 8,000+ apps, \$235B+ in total merchant sales



Store Setup

Theme selection, product management, collections, Shopify admin, and Online Store editor



Shopify vs. Woo

Shopify: speed and simplicity (\$39+/mo); WooCommerce: budget and full customization (free)



Morocco Context

Shopify best for export brands; WooCommerce best for local market with COD and MAD

Session Objectives

- 01** Understand how online payment systems work: gateways, processors, and merchant accounts
- 02** Master e-commerce security fundamentals: SSL, HTTPS, encryption, and PCI DSS compliance
- 03** Identify common fraud types and implement prevention strategies for online stores
- 04** Compare payment solutions available in Morocco: CMI, cash on delivery, and mobile wallets
- 05** Build customer trust through security badges, transparent policies, and secure checkout

Agenda: Payment Systems → Security & Fraud → Trust & Compliance → Morocco Focus → Implementation

How Online Payments Work

Every online purchase involves a chain of trust: the customer's bank authorizes payment, a processor routes it, and funds reach the merchant — all in under 3 seconds.



Payment Gateway

The front door — captures card details securely, encrypts them, and sends to the processor



Payment Processor

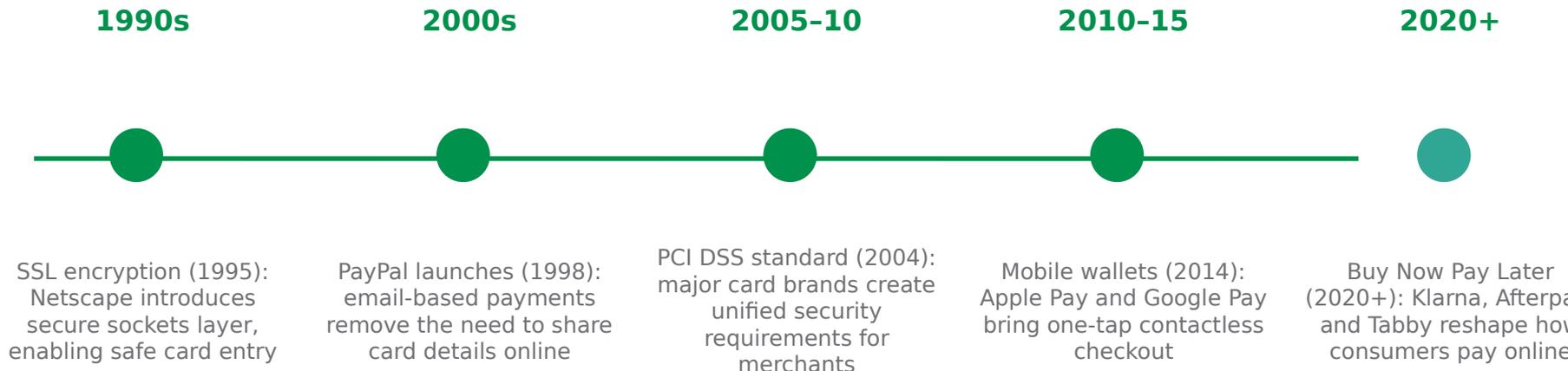
The engine — routes transactions between issuing bank, card network, and acquiring bank



Merchant Account

The destination — holds funds before settlement to the merchant's business bank account

Evolution of Online Payments



Global digital payment transactions exceeded \$9.5 trillion in 2023 — cash is rapidly declining

Payment & Security by the Numbers

\$9.5T

Global Digital Payment Transactions (2023)

\$48B

E-Commerce Fraud Losses (Annual)

82%

of Shoppers Check for SSL Before Buying

60%+

Morocco Orders Paid by COD

Payment Methods Overview



**Credit & Debit /
Cards**



**Digital Wallets /
PayPal, Apple Pay**



**Payment
Methods**



**Bank Transfer /
Wire, SEPA**



**Cash on /
Delivery (COD)**



**Offering multiple payment
methods increases
conversion — 50% of
buyers abandon if their
method is missing**

Security Fundamentals

SSL / TLS Certificates

Encrypts data between browser and server — the padlock icon and HTTPS that customers look for

PCI DSS Compliance

12 requirements for handling card data — most stores achieve compliance via their payment gateway

Data Encryption

AES-256 encryption protects stored data; tokenization replaces card numbers with random tokens

Two-Factor Authentication

2FA on admin accounts prevents unauthorized access even if passwords are compromised



Morocco Security Context

- Law 09-08 (CNDP) governs personal data protection in Morocco
- Free SSL via Let's Encrypt — no excuse for unencrypted Moroccan stores
- CMI gateway handles PCI compliance for Moroccan merchants
- Bank Al-Maghrib regulates online payment security standards
- COD reduces online fraud risk but increases delivery refusal rates

Common E-Commerce Fraud Types



Card Fraud

Stolen card numbers used for purchases — the #1 fraud type, costing merchants \$48B annually



Friendly Fraud

Legitimate buyers dispute charges after receiving goods — chargebacks cost 2-3x the order value



Phishing Attacks

Fake emails or websites trick customers into entering credentials — damages brand trust



Morocco Fraud Reality

COD fraud: fake orders and delivery refusals • Card fraud growing with online adoption • Phone verification helps reduce fake orders • 3D Secure mandatory for CMI transactions

Fraud Prevention Strategies



3D Secure / SCA

Bank verification step during checkout — shifts fraud liability from merchant to card issuer



AVS & CVV Checks

Address Verification System and card security code matching — blocks mismatched card data



Fraud Detection Tools

Shopify Fraud Protect, Signifyd, Riskified — AI-powered tools that score transaction risk



Order Verification

Phone/SMS verification for COD orders — reduces fake orders by 40-60% in Morocco



Key Insight: In Morocco, implement phone verification for COD, enable 3D Secure for card payments, and use IP geolocation to flag suspicious orders from unexpected locations.

Building Customer Trust



SSL Badge & HTTPS

The padlock icon is non-negotiable — 82% of shoppers check for SSL before entering card details



Payment Badges

Display Visa, Mastercard, PayPal, and COD logos at checkout — familiar brands reduce anxiety



Return Policy

Clear, visible return and refund policies — 67% of shoppers check the return policy before buying



Customer Reviews

Verified purchase reviews and star ratings — 93% of buyers read reviews before making a purchase



Privacy Policy

GDPR and Morocco Law 09-08 compliant privacy policy — required by law and expected by customers



Contact Information

Visible phone number, email, and physical address — real contact info builds legitimacy

Payment Gateway Comparison



Stripe

Developer-friendly, 135+ currencies, 2.9% + \$0.30 per transaction — not directly available in Morocco



PayPal

300M+ users globally, buyer protection, 2.9% + fixed fee — available in Morocco for international payments



CMI (Morocco)

Centre Monétique Interbancaire — Morocco's national gateway for local bank cards, 3D Secure enabled



Shopify Payments

Built-in for Shopify stores, no extra fees, 2.9% + \$0.30 — not yet available in Morocco



Morocco Payments

CMI for local cards + PayPal for international + COD for trust — the Moroccan payment trifecta



Gateway Rule

Always offer 3+ payment methods — each missing option costs you 5-10% of potential conversions

Compliance Requirements



PCI DSS

Payment Card Industry standard — 12 requirements for secure card handling; use hosted gateways to simplify



GDPR (Europe)

General Data Protection Regulation — applies if you sell to EU customers; consent and data rights



Law 09-08 (Morocco)

Morocco's data protection law enforced by CNDP — registration required for collecting personal data



Consumer Protection

Law 31-08 in Morocco — right of withdrawal (7 days), transparent pricing, clear terms of sale



Morocco: register with CNDP, display legal mentions, honor 7-day withdrawal right (Law 31-08)

Payment & Security — Key Trade-offs

BENEFITS

- ✓ Multiple payment options increase conversion rates by 20-30%
- ✓ SSL certificates are free via Let's Encrypt — no cost barrier to HTTPS
- ✓ 3D Secure shifts fraud liability from merchant to card issuer
- ✓ Hosted payment gateways handle PCI compliance for you
- ✓ Trust badges increase checkout conversion by 15-20%
- ✓ COD eliminates online payment risk for cautious Moroccan shoppers
- ✓ Phone verification reduces COD fraud by 40-60% in Morocco

CHALLENGES

- ✗ Payment gateway fees (2-3% per transaction) eat into margins
- ✗ 3D Secure adds friction — 10-15% of customers drop off at verification
- ✗ PCI compliance is complex for stores handling card data directly
- ✗ COD has 15-30% delivery refusal rate — failed deliveries cost money
- ✗ Chargebacks cost 2-3x the order value including fees and penalties
- ✗ Fraud detection tools add monthly costs (\$50-500/mo for AI solutions)
- ✗ Morocco has limited gateway options — CMI and PayPal are the main choices

Payments & Security in Morocco

60%+

Orders Paid
Cash on Delivery

3D Secure

Mandatory for
CMI Transactions

CNDP

Data Protection
Authority (Law 09-08)

Payment Landscape

- CMI is the only national gateway for Moroccan bank cards — requires merchant registration
- PayPal is available for international transactions — widely used by export-focused stores
- Mobile wallets (M-Wallet, Inwi Money) are emerging but adoption remains low
- COD dominates due to low card penetration and trust issues with online payments
- Morocco Digital 2030 aims to triple online payment adoption through financial inclusion programs

Your Payment & Security Checklist



1. Enable SSL/HTTPS

Install SSL certificate (free via Let's Encrypt) — force HTTPS on all pages, especially checkout



2. Set Up Payments

Enable COD + CMI for local cards + PayPal for international — offer 3+ methods minimum



3. Add Fraud Prevention

Enable 3D Secure, phone verification for COD, and install fraud detection on high-risk orders



4. Build Trust

Add SSL badge, payment logos, return policy, privacy policy, and visible contact information

Payment & Security Success Stories



Amazon: 1-Click Payment

Patented 1-Click reduced checkout friction to zero — stored payment and address drove billions in extra sales



Stripe: Developer-First

Built a \$95B company by making payments integration simple for developers — 7 lines of code to accept payments



Jumia Morocco: COD + Cards

Offers both COD and CMI card payments — phone verification reduced fake COD orders by 50% in key cities



Klarna: Buy Now Pay Later

BNPL increased average order value by 45% for partner merchants — installment payments reduce purchase hesitation



Key Takeaways

- 1 Online payment flows through gateway, processor, and merchant account — each step must be secure
- 2 SSL/HTTPS is non-negotiable — 82% of shoppers check for the padlock before entering card details
- 3 E-commerce fraud costs \$48B annually — use 3D Secure, AVS, CVV checks, and AI fraud detection
- 4 Trust signals (badges, reviews, return policies, contact info) increase conversion by 15-20%
- 5 In Morocco, offer COD + CMI + PayPal, comply with CNDP (Law 09-08), and verify COD orders by phone



Homework & Required Reading

Required Reading

Book: *"How to design, create, and manage your site"*

Author: Pelet, Jean-Eric | **Publisher:** Dunod (2018)

Pages: 161 to 180

Access: <http://international.scholarvox.com>

Coming Up — Session 12

Trends and Perspectives in E-Commerce — We will identify future developments in e-commerce, understand the impact of mobile commerce, social commerce, AI, and omnichannel.

Thank you | Questions? | See you next session!