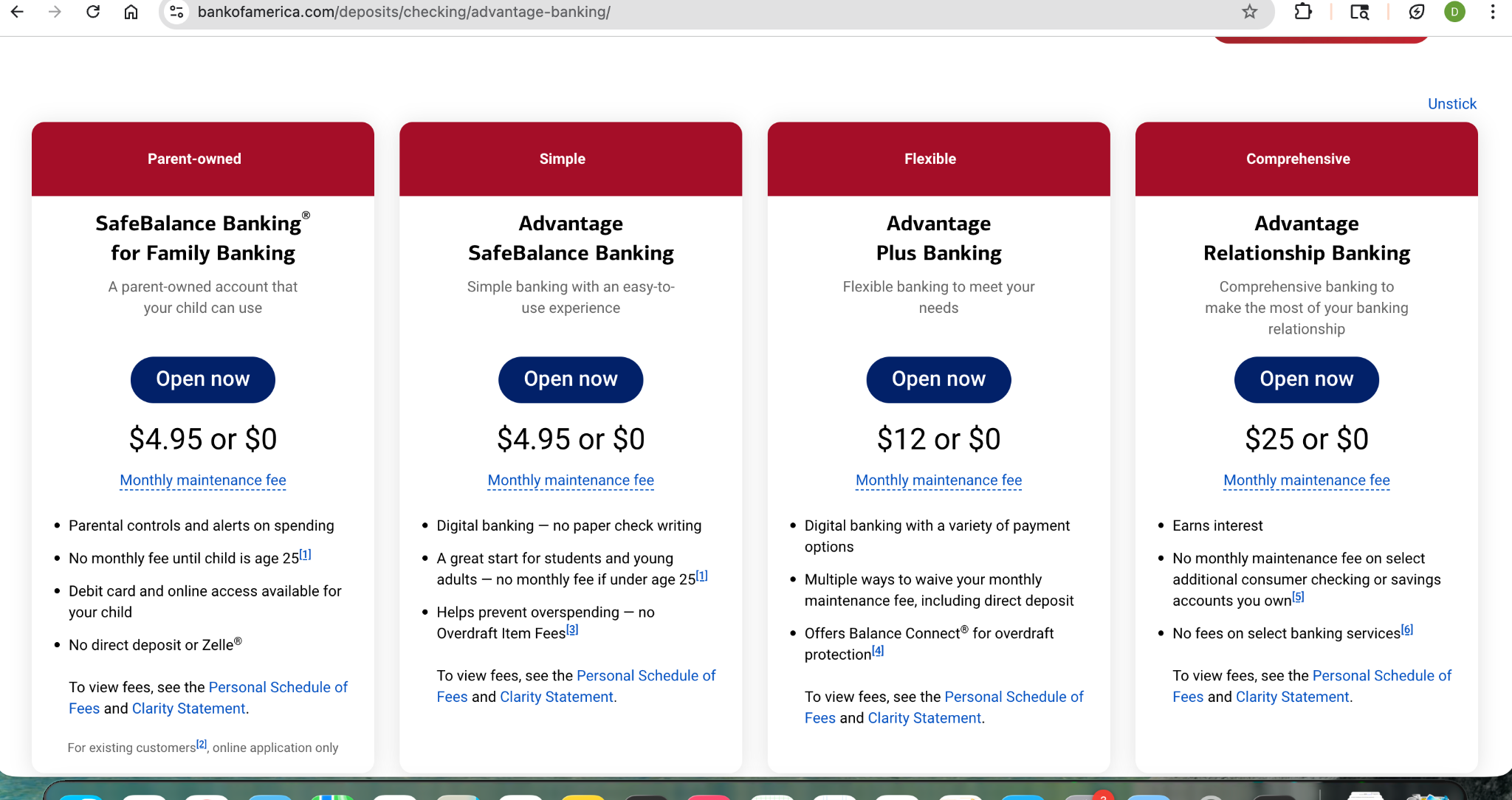
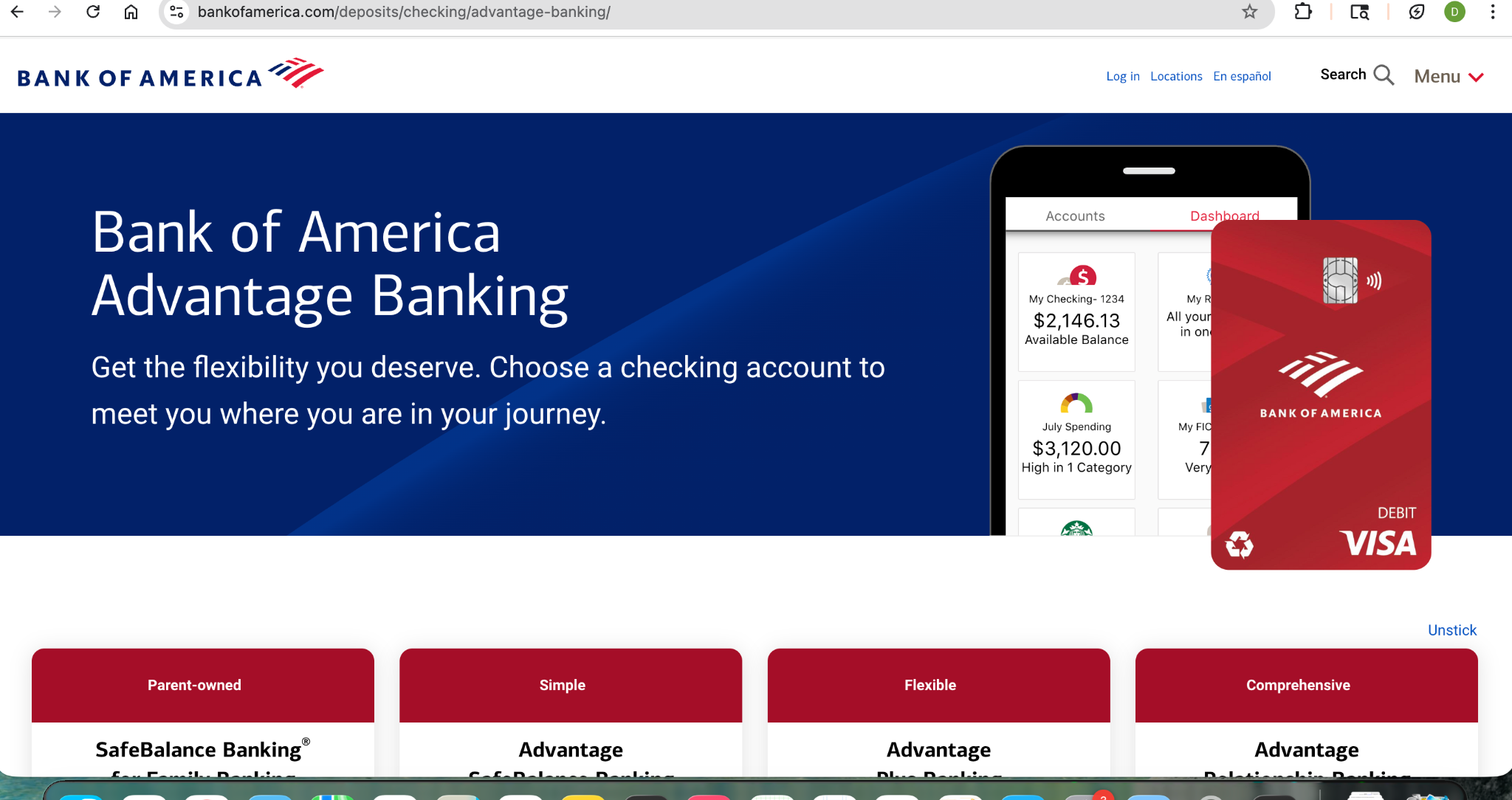


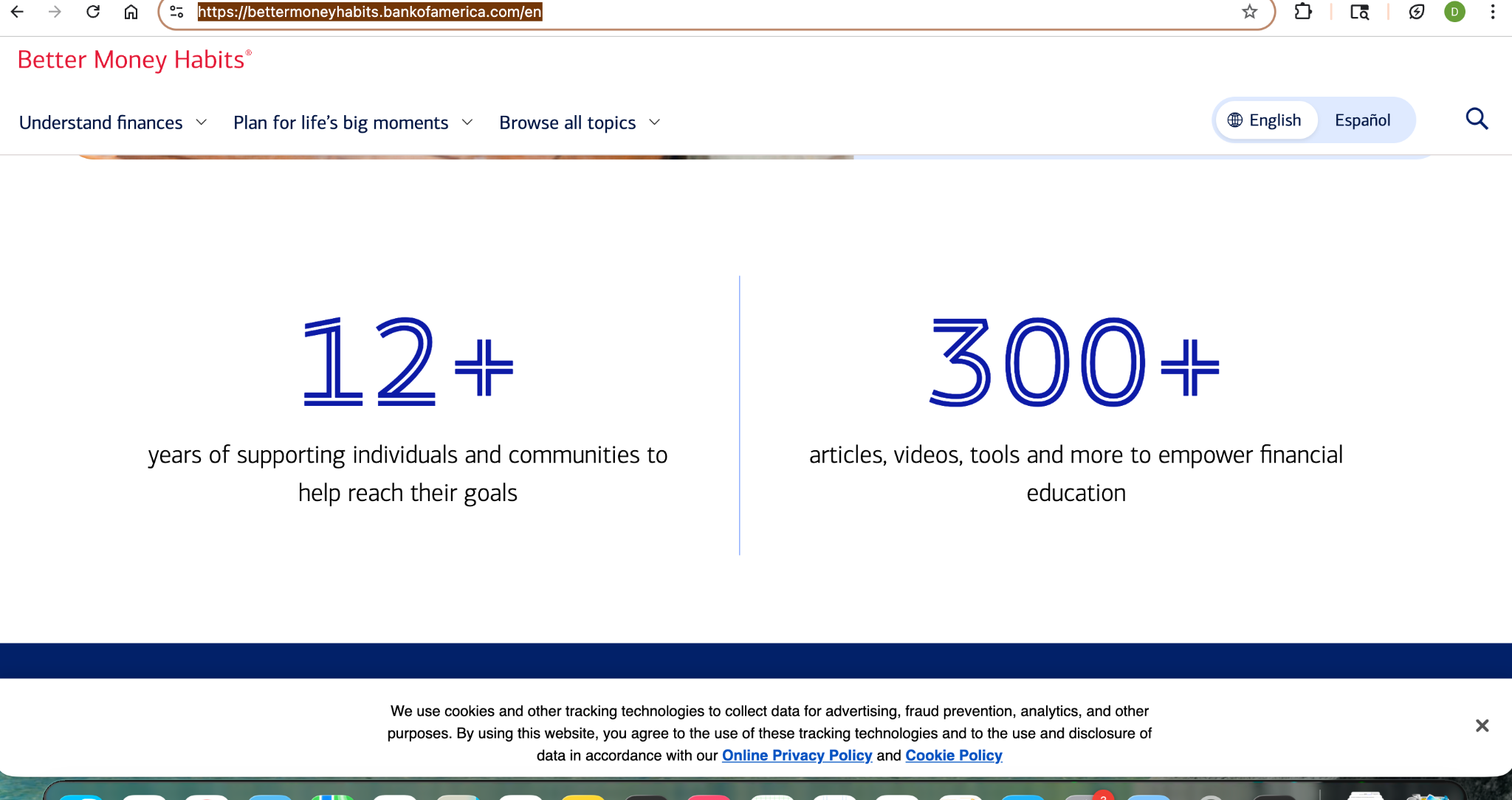
I like Bank of America’s website, very easy to read, clean and organized. Looks accessible for every level of person and company. Not AI or futuristic looking. Not too much scrolling on each page.

<https://www.bankofamerica.com/deposits/checking/advantage-banking/>

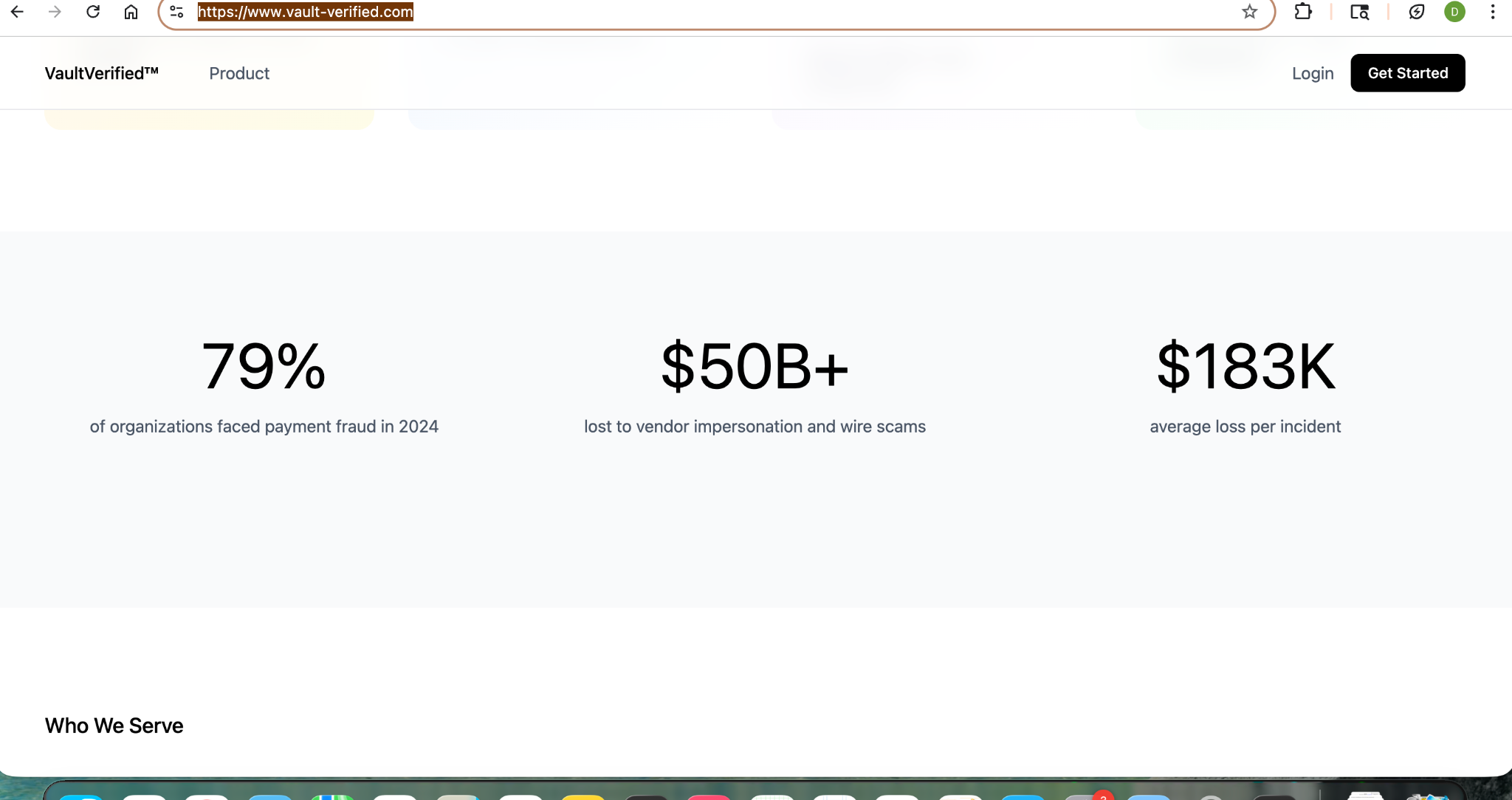
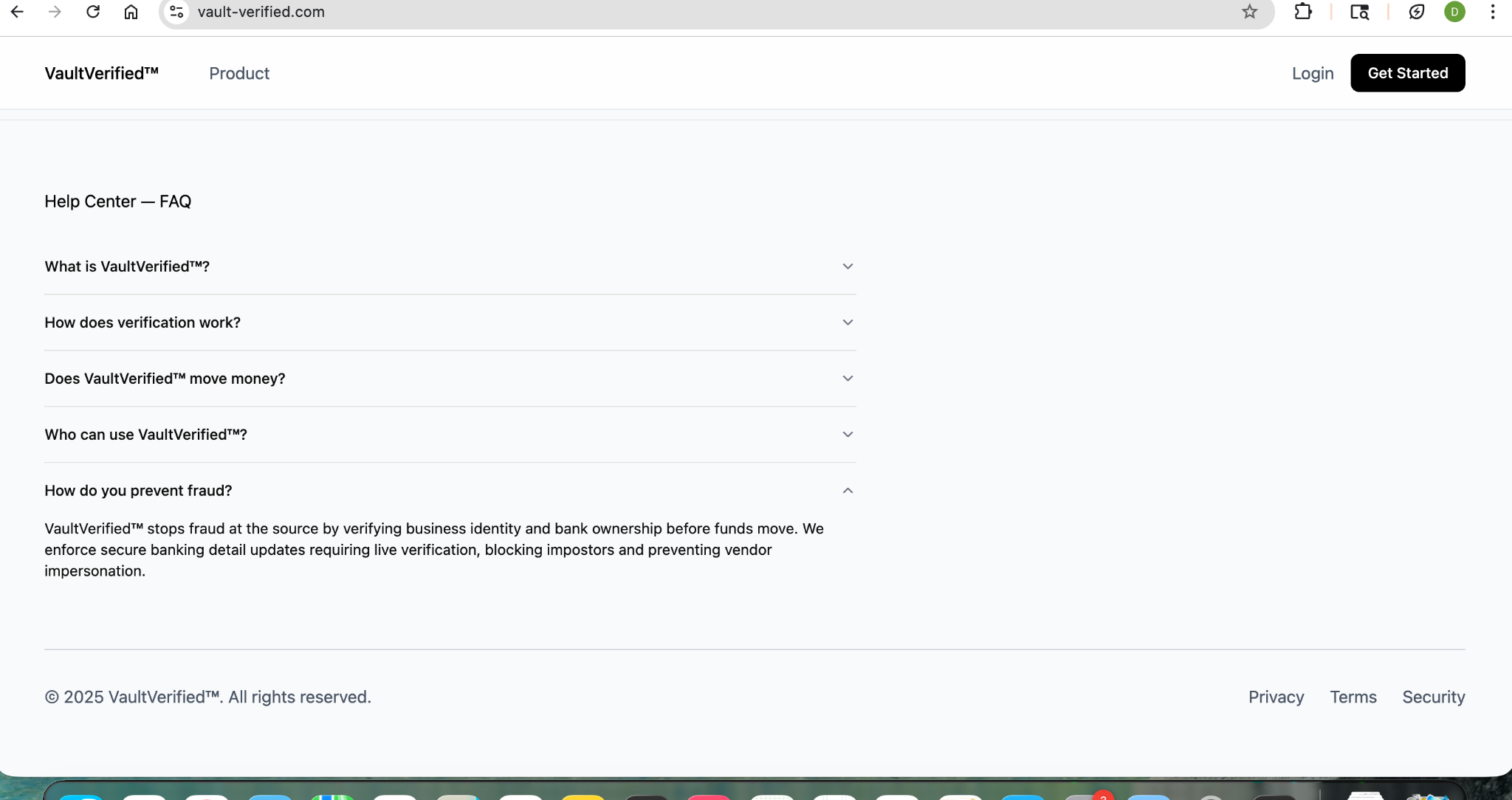
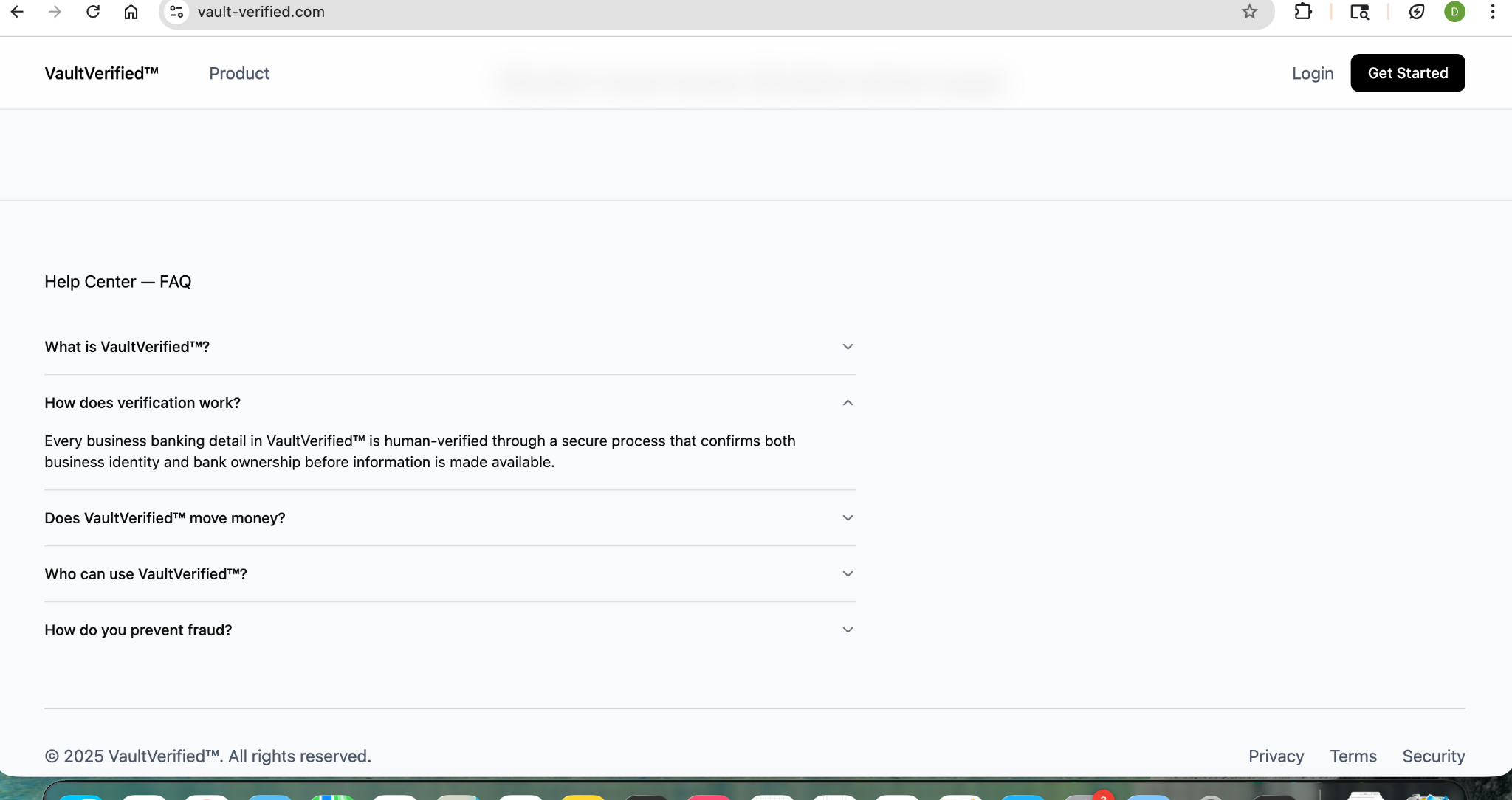
<https://promotions.bankofamerica.com/homeloans/homeresourcecenter/preparingtobuy?subCampCode=94362&dmcode=18098621553>

<https://bettermoneyhabits.bankofamerica.com/en>





[https://www.vault-verified.com](https://www.vault-verified.com/)/



# 

# 

# 

# 

# 

# 

# 

# 

# 

# **VaultVerified — Official Website Structure & Core Content (v1)**

**Purpose of this document** This file is meant to give the development + design team a *clear strategic understanding* of **what VaultVerified is**, **why it exists**, **what problems it solves**, and **how the website should be structured and flow**.

## **1. Core Message & WHY This Matters**

### **The Problem We Exist to Solve**

Modern payment fraud is **not random** and **not caused by careless employees**.

Fraud today happens because:

* Attackers gain access to **legitimate corporate email accounts**
* They **impersonate real employees from inside the email system**
* They silently create **email rules** that reroute or hide messages
* They observe invoice timing, vendor relationships, approval flows
* They wait until the *perfect moment* to redirect payments

This is **Business Email Compromise (BEC)**.

Traditional controls fail because:

* Email itself is treated as a trusted channel
* Banking changes are approved via email and phone calls
* Identity is assumed, not proven
* Compliance focuses on documentation *after* the damage is done

### **VaultVerified’s Philosophy**

**Email should never be a system of record for money.**

VaultVerified removes sensitive financial actions from email entirely and replaces them with:

* Verified identity
* Secure workflows
* Real-time validation
* Documented audit trails

We do not just *detect* fraud — we **eliminate the conditions that allow it to happen**.

## **2. What Makes VaultVerified Different (High-Level Pillars)**

These concepts should subtly guide design, spacing, and hierarchy:

1. **Prevention over reaction**
2. **Identity over intent**
3. **Process over policy**
4. **Trust through verification**
5. **Compliance built-in, not bolted-on**

The site should feel:

* Calm
* Authoritative
* Structured
* Non-alarmist
* Enterprise-grade

No hype. No fear tactics. Just clarity.

## **3. Website Architecture (Top-Level Navigation)**

**Primary Nav**

* Home
* Solutions
  + Vault (Secure Banking Updates)
  + NACHA Compliance & Audit
  + Outsourced Verification / Fraud Department (VAAS)
* Resources
* Company
* Contact

**Persistent CTAs**

* Request a Demo
* Sign Up

## **4. HOME PAGE — STRUCTURE & DRAFT CONTENT**

### **Section 1: Hero (Above the Fold)**

**Primary Message:**

Secure payment changes. Verified identity. Built-in compliance.

**Subtext:**

VaultVerified prevents ACH and wire fraud by removing banking changes from email, verifying real identities, and creating an auditable, compliant verification process.

**CTAs:**

* Request a Demo
* Get Started

### **Section 2: Why Fraud Happens (Education First)**

**Headline:**

Fraud doesn’t start with a bad actor — it starts with a trusted email.

**Content (Your Definition — Editable):**

Fraud happens after someone gains access to your email system.

Attackers impersonate real employees **from inside their actual email accounts**. They create rules that route messages away from the inbox, allowing them to sit silently inside the organization.

They watch:

* Vendor communications
* Invoice timing
* Approval patterns
* Payment schedules

At the right moment, they send instructions — using your real email — to redirect funds to accounts they control.

By the time fraud is detected, the transaction is complete.

### **Section 3: The Core Failure**

**Headline:**

Email was never meant to be a financial system.

**Key Points:**

* Banking changes sent via email cannot be trusted
* Identity is assumed, not verified
* Approvals lack audit-grade evidence
* Compliance requirements are increasing

VaultVerified removes email from the equation.

### **Section 4: How VaultVerified Works (High-Level)**

**Three Pillars (Visual Cards):**

**1. Secure Banking Vault**Real-time banking information and updates — never exchanged via email.

**2. NACHA-Compliant Verification**Documented identity verification and reporting aligned with evolving standards.

**3. Outsourced Verification & Fraud Operations**A dedicated verification function without hiring or scaling internal teams.

CTA: View Solutions

## **5. SOLUTIONS OVERVIEW PAGE**

### **Intro**

Modular solutions designed to eliminate payment fraud, enforce verification, and meet compliance requirements — without disrupting operations.

### **Solution 1: Vault — Secure Banking Information**

**Short Description:**

A secure system for managing banking information and payment updates — without email, PDFs, or manual verification.

CTA: Learn More

### **Solution 2: NACHA Compliance & Audit Readiness**

**Short Description:**

Identity verification, documentation, and reporting aligned with NACHA requirements — including March 2026 updates.

CTA: Learn More

### **Solution 3: Outsourced Verification / Fraud Department (VAAS)**

**Short Description:**

Verification-as-a-Service for organizations that want expert oversight without building an internal fraud team.

CTA: Learn More

## **6. VAULT PAGE — 5 Ws STRUCTURE**

### **What Is the Vault?**

A secure platform for storing and updating banking information outside of email.

### **Who Is It For?**

* AP teams
* Finance teams
* Security & risk leaders
* Organizations processing ACH and wire payments

### **Why We Built It**

Because email-based banking changes are the #1 entry point for BEC (business email compromise) fraud.

### **Where Is Data Stored?**

Secure, access-controlled infrastructure with full logging and traceability.

### **When Is Information Available?**

Real-time updates with immediate validation and visibility.

## **7. NACHA PAGE — EDUCATION + PROCESS**

### **Section 1: What’s Changing (March 2026)**

* Stronger identity verification expectations
* Increased audit and documentation requirements
* Greater accountability for originators

### **Section 2: Why This Matters**

Compliance is no longer optional or passive.

Organizations must be able to **prove**:

* Who was verified
* How they were verified
* When verification occurred
* What controls were used

### **Section 3: How VaultVerified Meets NACHA Standards**

* Documented verification workflows
* Identity validation steps
* Time-stamped audit trails
* Exportable compliance reporting

## **8. OUTSOURCED VERIFICATION / FRAUD DEPARTMENT (VAAS)**

### **What Is VAAS?**

Verification-as-a-Service provides a dedicated fraud and verification function without internal hiring.

### **What We Handle**

* Banking change verification
* Identity validation
* Vendor communication oversight
* Exception handling
* Documentation and reporting

### **Why Organizations Use VAAS**

* Reduce internal workload
* Eliminate verification gaps
* Scale without headcount
* Gain expert oversight

## **9. RESOURCES**

**Categories:**

* Blog
* Articles
* Case Studies
* How-To Guides (Vault usage)

Purpose: Education, trust, and authority.

## **10. COMPANY PAGE**

### **Our Mission**

To eliminate payment fraud by replacing trust assumptions with verified identity and secure processes.

### **Our Philosophy**

Fraud prevention should be built into systems — not left to individuals.

## **11. CONTACT US PAGE**

* Contact form
* Support
* Demo requests
* Sign Up