Guard Your Card: Protecting Your Private Data

EPC Electronic Payments Coalition

Credit cards provide top-tier security and convenience for consumers and businesses, but the Durbin-Marshall credit card mandates put this robust system at risk. By forcing transactions onto untested and unknown networks, these mandates weaken fraud protections, exposing consumers' private data and threatening security, all to boost profits for corporate megastores.

A Payments System That Works

Credit cards deliver peace of mind, alerting consumers to fraud attempts **with 96% of all fraud cases being blocked or refunded. Payments industry leaders invest a staggering $22 billion annually** to protect consumer data with advanced AI and fraud detection tools, safeguarding families, small businesses, and the economy.

The Rising Threat of Fraud

Hackers and data breaches are a constant, increasing threat. Financial institutions are always on alert and improving their systems to fight back to protect their customers.

- **Debit fraud attempts are up 124%** following Durbin 1.0 debit card mandates.
- Nearly 800,000 **records are lost to hacking each day**, about two-thirds through office and business applications.
- **Online scams cost consumers $1 trillion globally** in 2024, according to a report from Feedzai.

Payments Industry: Billions For Safety

Payment leaders are on the front lines to protect consumers against fraudsters leveraging AI-driven phishing, deepfake scams and more. Visa, for example, **has invested $12 billion over five years and disrupted $350 million in fraud** in 2024. Its scam detection team, blending cybersecurity and law enforcement expertise, **took down 12,000 fraudulent merchant sites** last year, **saving $27 million in losses**. Mastercard and others have followed suit, ensuring consumers' data stays safe, protected, and private.

Corporate Megastores: Profits Over Protection

While payment networks invest billions in security, corporate mega-stores cut corners, repeating past mistakes, ignoring lessons from past breaches, and ultimately placing profits ahead of consumer protection. This negligence has resulted in corporate megastores regularly falling victim to data breaches: **malware attacks at Wawa, Home Depot, and Target alone exposed the data of over 127 million cardholders**. In 2023, **corporate megastores' refusal to upgrade security systems cost the U.S. economy $12 billion**, as cybercriminals exploited weak defenses to commit card-not-present fraud, a top target for cybercriminals.

Durbin-Marshall: A Risk American's Cannot Afford

The Durbin-Marshall credit card mandates would give merchants the power to route transactions over cheaper, less secure and unknown networks, slashing the resources needed to fight fraud. Splitting transactions across networks weakens AI fraud detection, delaying response times and increasing risk.

Academic studies warn of the Durbin-Marshall consequences:

- **40% spike in fraud**, adding $6.40 per $10,000 in transactions annually.
- **Credit fraud could reach $20 billion by 2035**—doubling the 2021 levels.

Lawmakers should reject Durbin-Marshall — corporate profits should *never* come at the cost of Americans' security.

EPC is the voice of credit unions, community banks, payment card networks, and institutions who support the backbone of our economic system: electronic payments. Learn more at ElectronicPaymentsCoalition.org.

EPC Electronic Payments Coalition