SECURE PAYMENTS PARTNERSHIP

FMI THE VOICE OF FOOD RETAIL   NACS   NGA NATIONAL GROCERS ASSOCIATION   NRF NATIONAL RETAIL FEDERATION   SHAZAM   PCA PREMIUM CIGAR ASSOCIATION
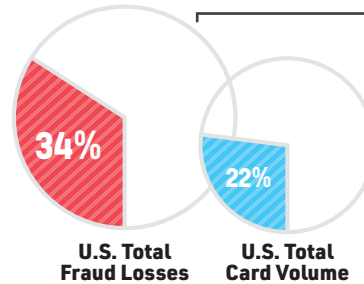
U.S. PAYMENT CARDS LEAD THE WORLD IN FRAUD

ONE THIRD
One third (33.6%) of the world's credit card fraud happens in the U.S. *(The Nilson Report, 2020)*

OVER $9 BILLION
U.S. payment cards accounted for over $9 billion of fraud in 2019 *(Nilson Report, 2020)*

34%
U.S. Total Fraud Losses

22%
U.S. Total Card Volume

IN THE U.S.
The U.S. accounted for 22% of total card volume worldwide yet 34% of gross card fraud losses worldwide in 2019.

WE NEED TO IMPROVE PAYMENT SECURITY IN THE U.S.

THE PAYMENT SYSTEM DEPENDS ON MULTIPLE PLAYERS ACROSS MULTIPLE INDUSTRIES

Payments travel through a complex network that requires multiple industries to interact with each other in order to be successful. These transactions are governed by standards that determine how they interact. These protocols must work for everyone across the system.
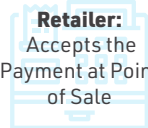
Device Manufacturer:
Enables Security Standards

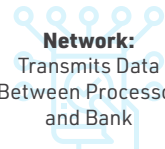**Retailer:**
Accepts the Payment at Point of Sale

Payments Processor:
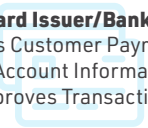Connects Retailers and Card Issuers to the Payment Network

Network:
Transmits Data Between Processor and Bank

Card Issuer/Bank:
Holds Customer Payment Card Account Information / Approves Transaction

SECURING THE PAYMENTS SYSTEM REQUIRES AN EQUAL PLAYING FIELD FOR ALL STAKEHOLDERS TO PARTICIPATE IN THE CREATION AND DEPLOYMENT OF PAYMENTS SECURITY STANDARDS

WHAT INNOVATIONS CAN HELP FIGHT PAYMENT FRAUD?

Technology advancements are being pioneered by companies throughout the payments system to combat fraud in-store, online, and via mobile transactions. Some of these innovations include:

Biometrics   Back-End Algorithms   Geolocation   Blockchain

Text-Message Codes   Ultrasonic Soundwaves   IP Verification   PIN

THESE AND OTHER INNOVATIVE SECURITY SOLUTIONS COULD BE DEVELOPED AND DEPLOYED MUCH QUICKER THROUGH AN OPEN AND COLLABORATIVE ENVIRONMENT

WHO WE ARE

The Secure Payments Partnership (SPP) is a coalition of companies and trade organizations that span the payments ecosystem with a collective interest in ensuring that the United States has the most innovative and secure payments system in the world.

Our payments system is rapidly evolving, and we must ensure that there are systems and guardrails in place that ensure security, foster competition, and enable real transparency as the world of payments changes.

By incorporating the voices of entities from across the payments spectrum, SPP has identified the following key principles that will help ensure that the United States leads the world in fast, secure, and transparent payments.

WHAT WE STAND FOR
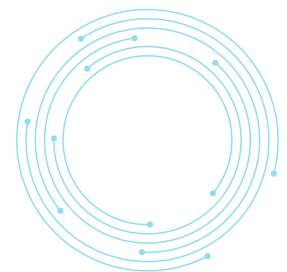
Strong User Authentication

To ensure the security of a transaction, we must be able to authenticate the identity of the person making a payment. There exist a variety of ways to do this both online and in-person. Unfortunately, very few of these methods have been approved or deployed by the card networks across the payments system.

In the near term we believe that PIN should be enabled on all payment cards, as it is in most of the rest of the world. But as new technologies become available, those advancements should be available online, in-store, and in mobile transactions.

Payments Security Innovation

Payment technologies take a lot of different forms, but we must always ensure that the payments system uses the best security technology available. SPP supports the use of innovative technologies that move the U.S. payments system forward, from biometrics to blockchain, and others that will make U.S. transactions the most secure in the world.

Open Security and Implementation Standards

The payment system is complex, made up of many participants, all of whom have expertise and should play a role in establishing payment card security standards and ensuring those standards are implemented fairly. Security standards and their implementation are important because they establish guidelines for anyone involved in the payment process from designing payment devices to accepting or processing payments.

Currently, these payment security standards are dictated by the Payment Card Industry Security Standards Council, a closed group controlled by one segment of the payment industry sector — the dominant payment card networks — and EMVCo, which is also controlled by the dominant payment card networks. And those payment networks also dictate the implementation of those standards. This closed decision-making process provides limited and non-voting opportunities for merchants, payment processors, and domestic debit networks to substantively shape the standards and policies governing payments transactions. This gives one narrow subset of the entire payments industry complete control over the creation and implementation of security standards that impact all businesses and consumers.

We must move beyond making decisions based on what is best for one business segment and enact standards and processes that benefit all members of the payment card industry and consumers.

Network Routing Competition

When a consumer swipes, dips, or taps their card, the network acts as a conduit through which that transaction is ultimately settled. While it is required that debit cards have multiple unaffiliated networks through which a transaction can be processed, credit cards only have one network option.

Multiple networks should be available on credit transactions as well. This will improve security, contain costs by promoting competition among networks, and ensure that a transaction can be processed even if one network is down.