fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

FELLSWAY | CELERANT | PAYROC — HOSTED BY NSSF

Securing Your Point of Sale System

Risk is constant. Ready is a choice.

fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

PANEL

Three lanes, one transaction

Steve Leventhal

CEO, Fellsway Group — **Moderator**

Jeff Warren

Lead Consultant, Fellsway Group — **The security lens**

Michele Salerno

Chief Growth Officer, Celerant — **The platform lens**

Laura Morgan

Account Executive, NE Region, Payroc — **The payments lens**

fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

TOPIC 1

What's actually sitting on your POS

💳 Payment data

Card transactions, every hour you're open

📋 Customer records

Names and identifiers tied to your 4473 and A&D recordkeeping

📦 Inventory and operations

What you have, what it's worth, where it sits

fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

TOPIC 2

How it actually goes wrong

It's rarely the terminal.

1 Remote access left open

Vendor and IT support tools, shared passwords, no multi-factor, running all the time

2 The back-office computer

One phished email on a machine that also touches the POS network

3 Systems past end of life

Known flaws, published fixes, nothing to apply them to

4 The register itself

Refunds, voids, and discounts with no second set of eyes

fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

TOPIC 3

Where does responsibility actually stop?

✅ Generally covered for you

- Encryption of card data inside a modern, validated terminal
- Security of the platform or hosted software itself
- Card brand network rules and processing infrastructure
- Product updates - published and made available to you

🚪 Stops at your door

- Who has a login, and whether those logins are shared
- Whether updates actually get installed on your machines
- Your network, your Wi-Fi, and everything else on it
- Physical security of readers and terminals
- Backups, and whether anyone has ever tested a restore
- Staff behavior — refunds, voids, discounts, cash handling

fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

TOPIC 4

Ten things you can verify this week

01

Every employee has a unique POS login

No shared manager code

02

Refunds, voids, and discounts need a second approval

Above a set threshold

03

Daily reconciliation

Reviewed by someone off the register

04

Multi-factor on every remote access path

Including your vendor's

05

Terminals do nothing but sell

No email, no browsing, no personal use

fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

TOPIC 4 — CONTINUED

Ten things you can verify this week

06

Your OS and POS software are still supported

And updates get installed

07

Card readers inspected on a schedule

Serial numbers logged

08

Guest Wi-Fi completely separate

From the POS network

09

Backups exist, are offline

And have been restored at least once

10

A written list of who to call

Processor, vendor, IT, insurance, counsel

fellsway

NSSF The Firearm Industry Trade Association

PROJECT CYBERSAFE

TOPIC 5

It just happened. Now what?

01 — Don't wipe it.

No reinstall, no factory reset. You destroy the evidence you'll need.

02 — Make the calls.

Processor, platform, security - in that order. Notification timelines are contractual.

03 — Decide if you can sell.

Know your manual fallback and its recordkeeping limits before you need it.

04 — Write it all down.

Times, symptoms, who you called, what you changed.

> The store that reopens Monday morning is the one that decided all of this in advance.

fellsway

NSSF
The Firearm Industry
Trade Association

PROJECT CYBERSAFE

Q+A

fellsway

NSSF
The Firearm Industry
Trade Association

PROJECT CYBERSAFE

Thank You!

Fellsway Group · Celerant · Payroc