BRINGING UP ISAC

- Spun off from Retail Industry Leaders Association (RILA) in 2014
- Seed funding from top retailers
- Operational in early 2015
- Currently at 85 members
- Board members include Target, Walgreens, JC Penney, AutoNation, Gap, Uphold, Levi Strauss & Co., RILA, MGM Resorts, TJX, and Lowe’s
WHAT COUNTS AS “RETAIL”? 

Traditional Retail

Non-Traditional Retail

Gaming, Sports, Media

Auto, Travel, Transit

Consumer Services

Hospitality, Lodging

Restaurant

Associates
TIGHT MARGINS

- No really, we mean TIGHT
DISPERSED ATTACK SURFACE
PHYSICAL SECURITY

Source: bbc.co.uk
TRANSACTION SPEED
THIRD PARTY RELATIONSHIPS
THE CUSTOMER IS THE ADVERSARY
FRAUD

- Tag-switching
- Fraudulent returns for gift cards
- Reshipping fraud
- Chargeback fraud
- Ad fraud
TRIANGULATION FRAUD

Sales site

Criminal

Posts picture of item for sale

Customer
TRIANGULATION FRAUD

Criminal

Sales site

Posts picture of item for sale

Customer

Purchases item
TRIANGULATION FRAUD

- Sales site
- Criminal $$$
- Customer
- Gets money
- Purchases item
TRIANGULATION FRAUD

Criminal

Uses stolen CC to order from retailer

Sales site

Retailer

Customer
TRIANGULATION FRAUD

Sales site

Criminal

$ $$

Retailer

Customer

Ships item to customer
OTHER TYPES OF FRAUD

Sales site
ACCOUNT TAKEOVER

- Automated account checkers
- Bulk account registration
- Reward points fraud
- Gift card fraud
- Shared customers = shared risks
CUSTOMER INFORMATION THEFT

• Anything used to “authenticate” the customer to the service rep
  • Example: Email account, mobile phone number
• Anything used to “authenticate” the service rep to the customer
  • Example: Dell service tag scam
• Not just “e-commerce” information, but any data relating to physical realm
• Assumption of physical proximity
SPEAKING OF AUTHENTICATION …

DISSED BY NIST
YOU’RE KIDDING, RIGHT?

• SMS will be the IE6 of 2FA for many years to come
AN EXAMPLE OF IOT THREAT MODELING

A SNEAKER THAT GIVES THE USER COMPLETE CREATIVE CONTROL

Watch Video
MAKESHIFT LABS SOFTWARE

With ShiftWear, you're connected to a real-time design marketplace featuring the hottest designers and animators. If your design catches on, the money goes to you. Save your favorite designs to your DisPlayList. Tag and share photos of your favorite ShiftWear looks, interacting with interesting and creative people from around the world! It's not just an App filled with designs, it's a social network! The software will allow you to Create and display your own images for free. You can also Buy and Sell other peoples designs.
FIRST ORDER OF BUSINESS

Shoes + downloadable designs + high school =

DRESS CODE VIOLATIONS
Hard to filter
Need to keep it running

With ShiftWear, you're connected to a real-time design marketplace featuring the hottest designers and animators. If your design catches on, the money goes to you. Save your favorite designs to your DisPlayList. Tag and share photos of your favorite ShiftWear looks, interacting with interesting and creative people from around the world! It's not just an App filled with designs, it's a social network! The software will allow you to Create and display your own images for free. You can also Buy and Sell other peoples designs.
Hard to filter
Need to keep it running

Direct monetization of fraud
Direct monetization of fraud

Hard to filter

Need to keep it running

Transmission channel for attacks
Direct monetization of fraud

Hard to filter

Need to keep it running

Transmission channel for attacks

Vulnerable software in multiple hostile environments
THE WHOLE PAYMENT QUESTION

• EMV
• Mobile payments
SUMMARY

• Physical access
• Remote access
• Crossover between cyber and fraud worlds