PaymentsEd FORUM

Your source for payments education

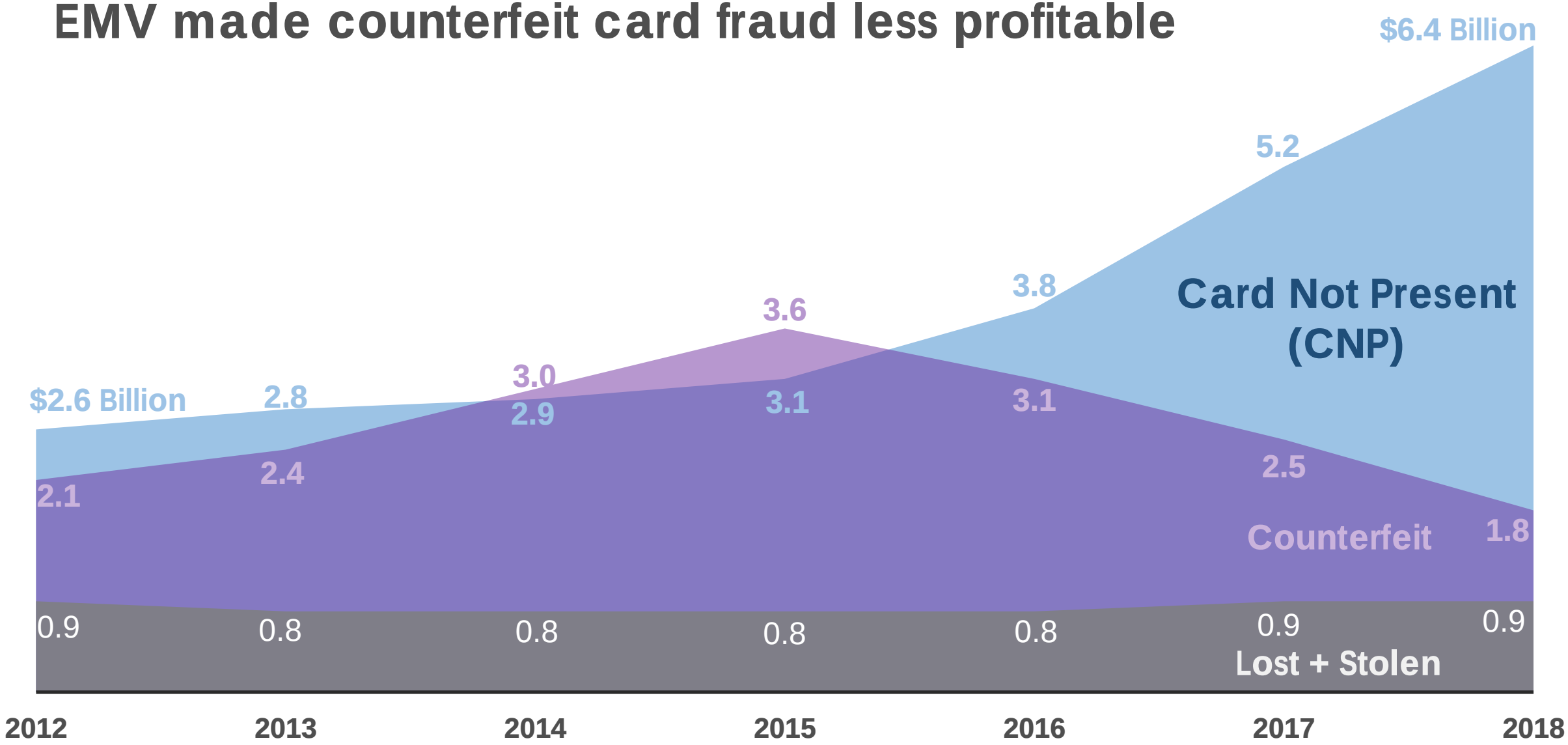
Authentication and Security in the Payments Ecosystem

Amy Zirkle, VP Industry Affairs, Electronic Transactions Association

What is driving Card Not Present fraud?

1. EMV made counterfeit card fraud less profitable
2. Data breaches have exposed billions of personal records, including financial data
3. Commerce is increasingly happening online (eCommerce)

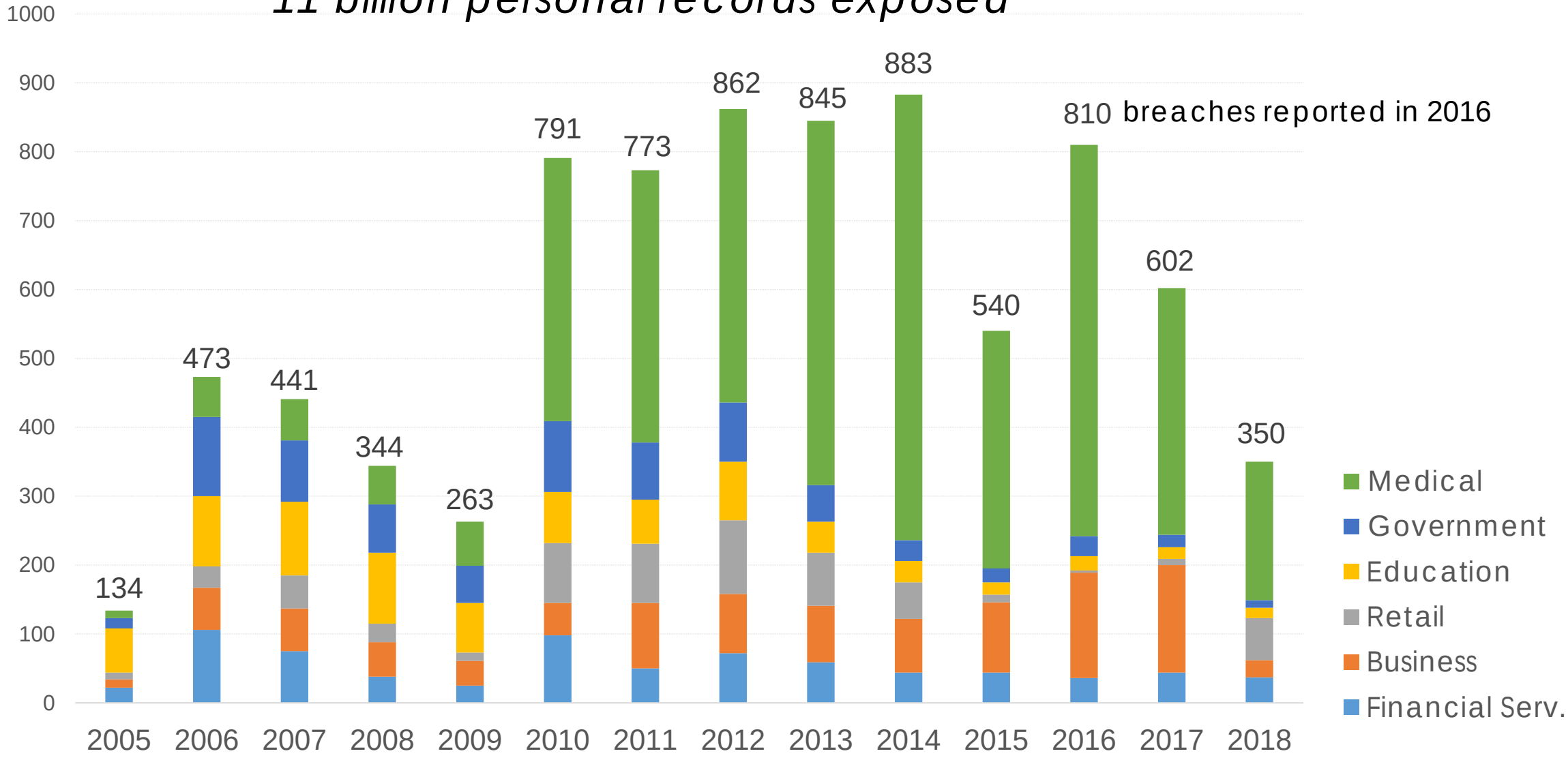
EMV made counterfeit card fraud less profitable



Data from Aite Group

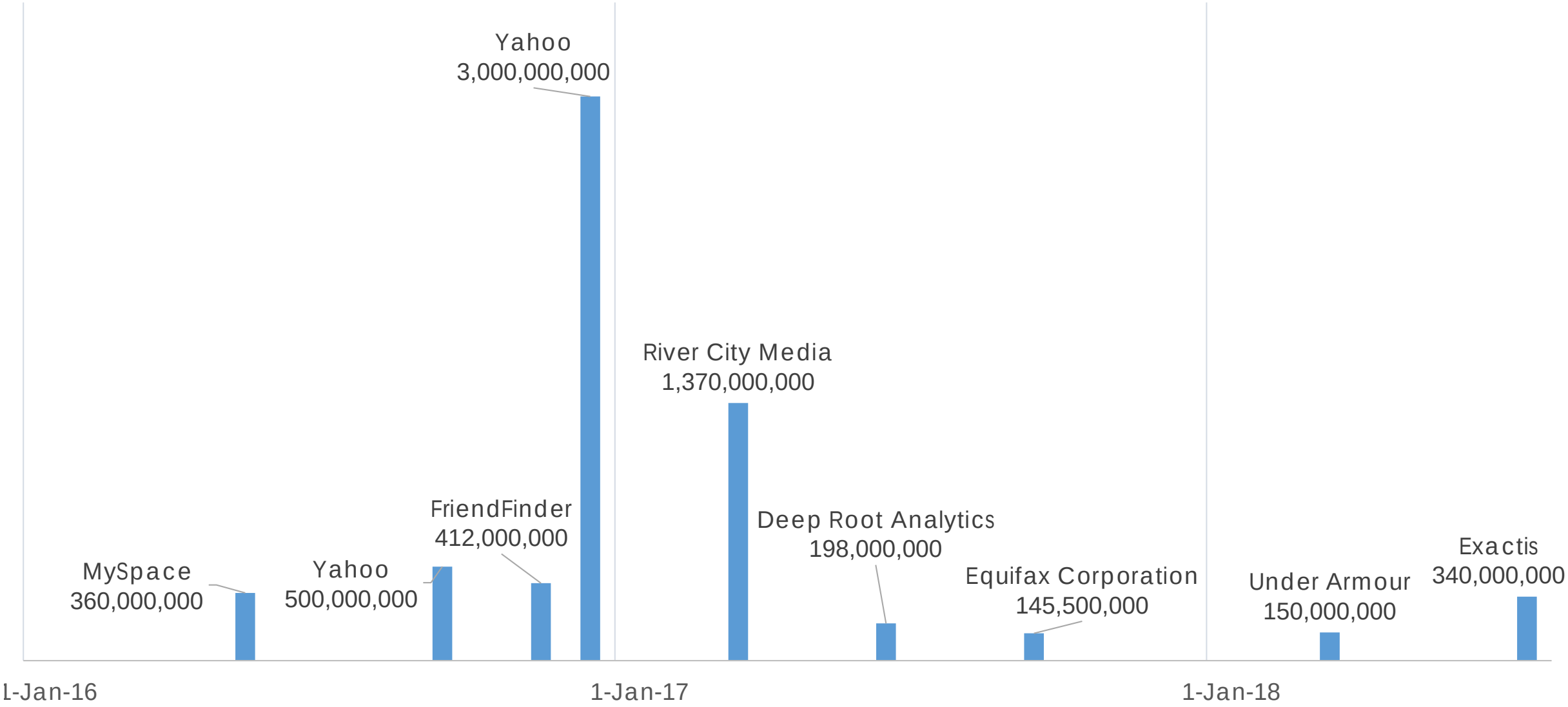
8000+ Data Breaches Reported Since 2005

11 billion personal records exposed



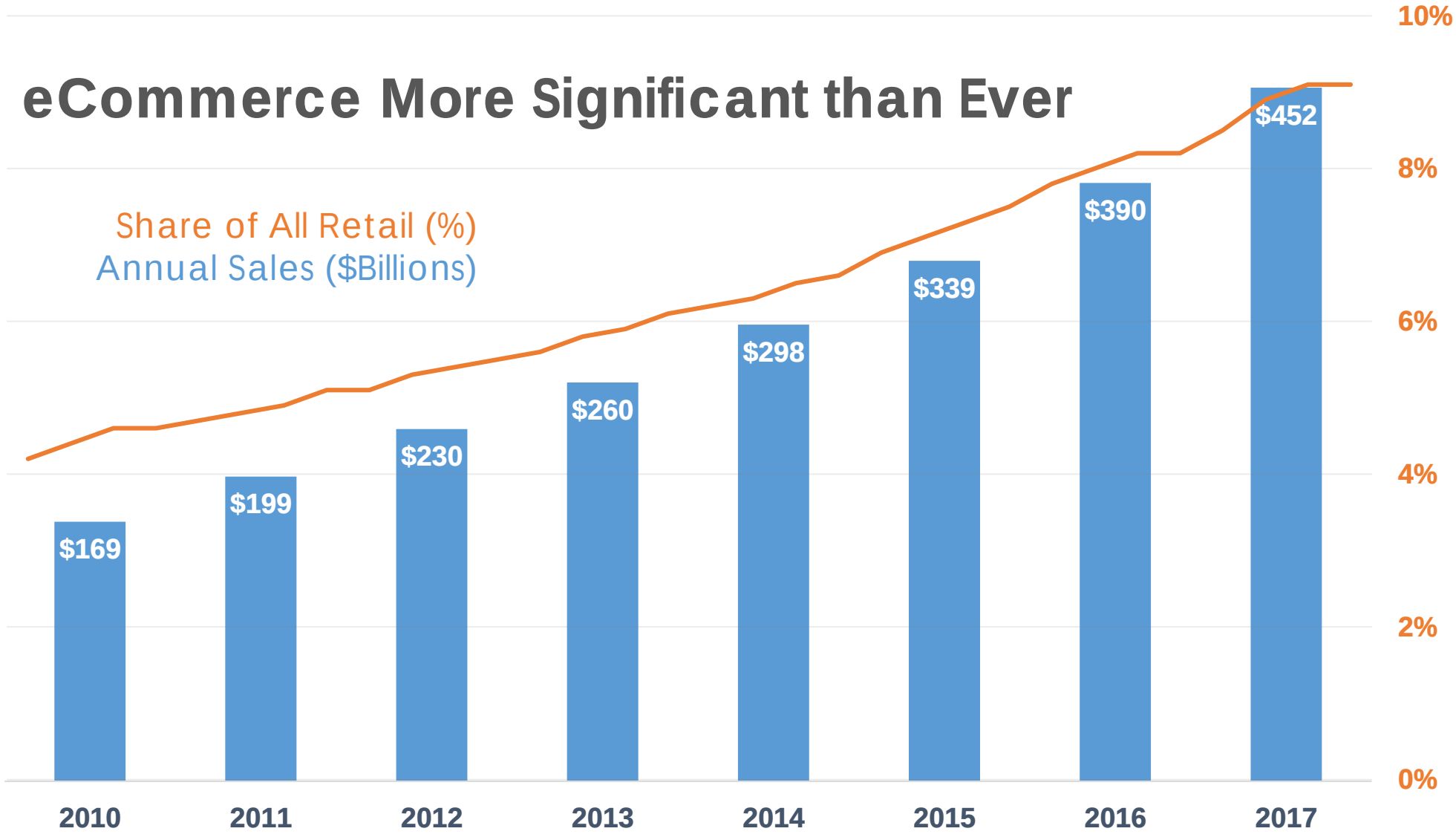
PaymentsEd FORUM

These 9 breaches alone have exposed **6.5 Billion** records



PaymentsEd FORUM

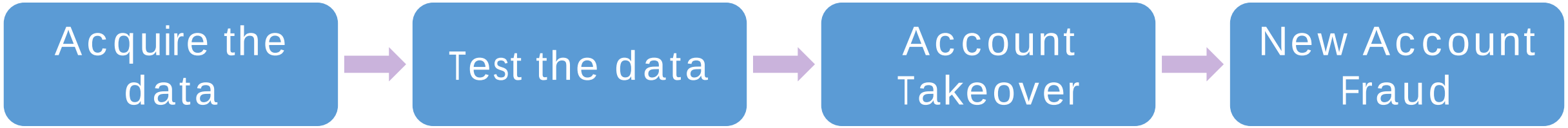
eCommerce More Significant than Ever



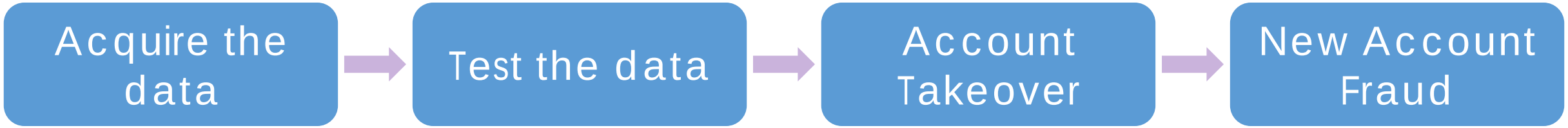
Data from the US Census Bureau and US Department of Commerce

PaymentsEd FORUM

Lifecycle of CNP Fraud

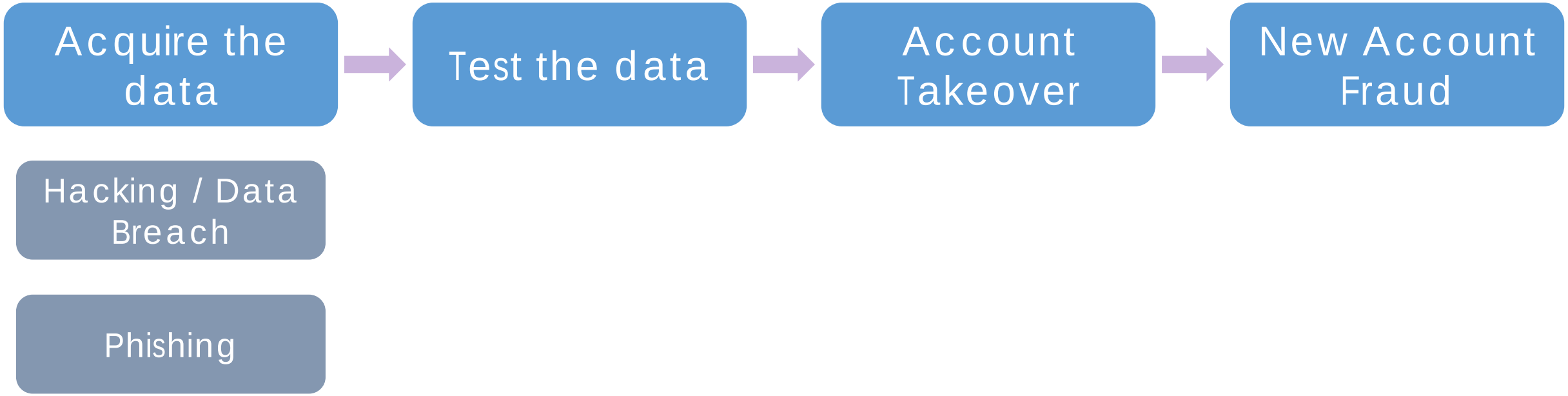


Lifecycle of CNP Fraud

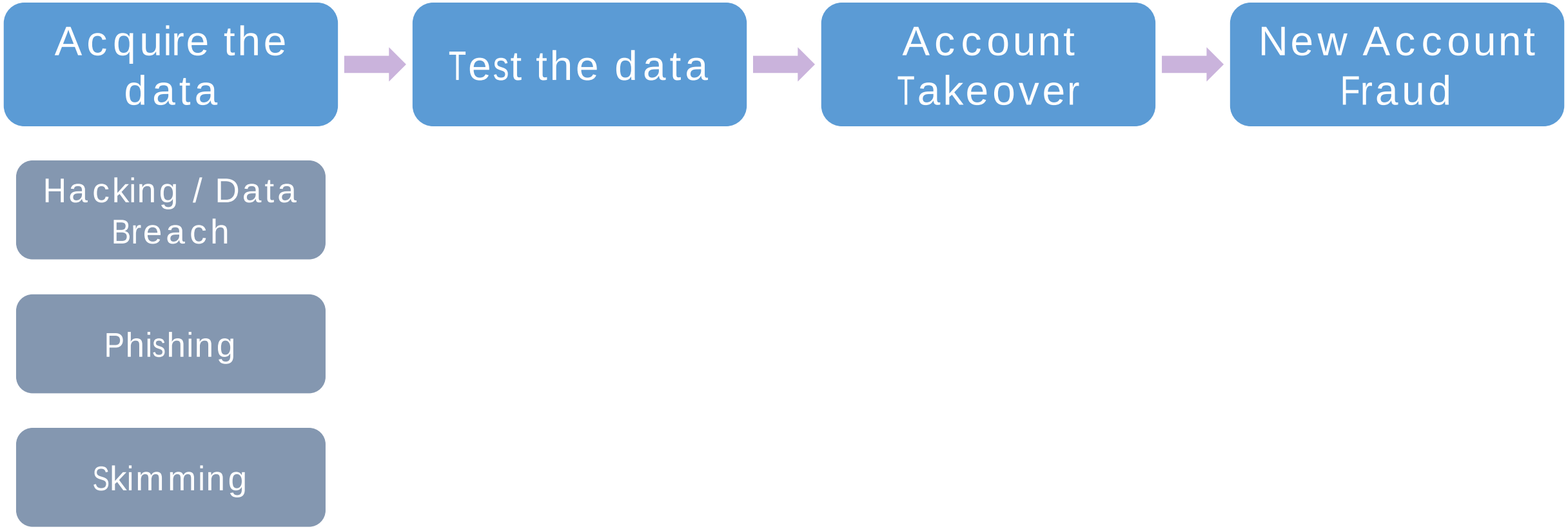


Hacking

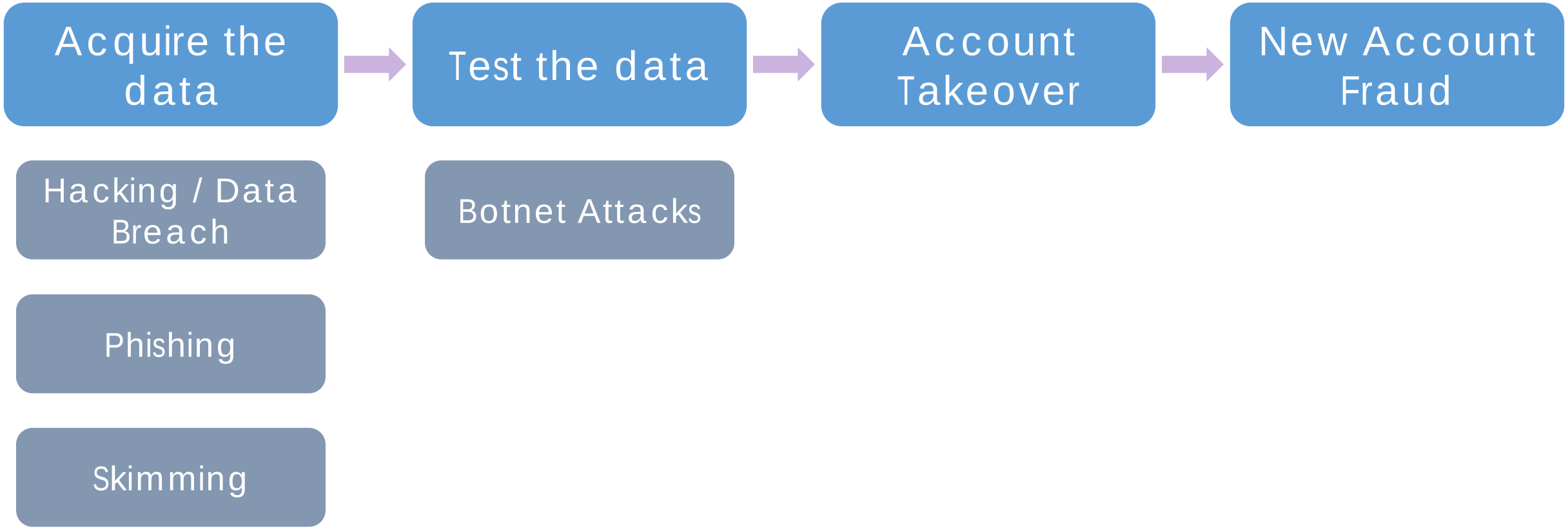
Lifecycle of CNP Fraud



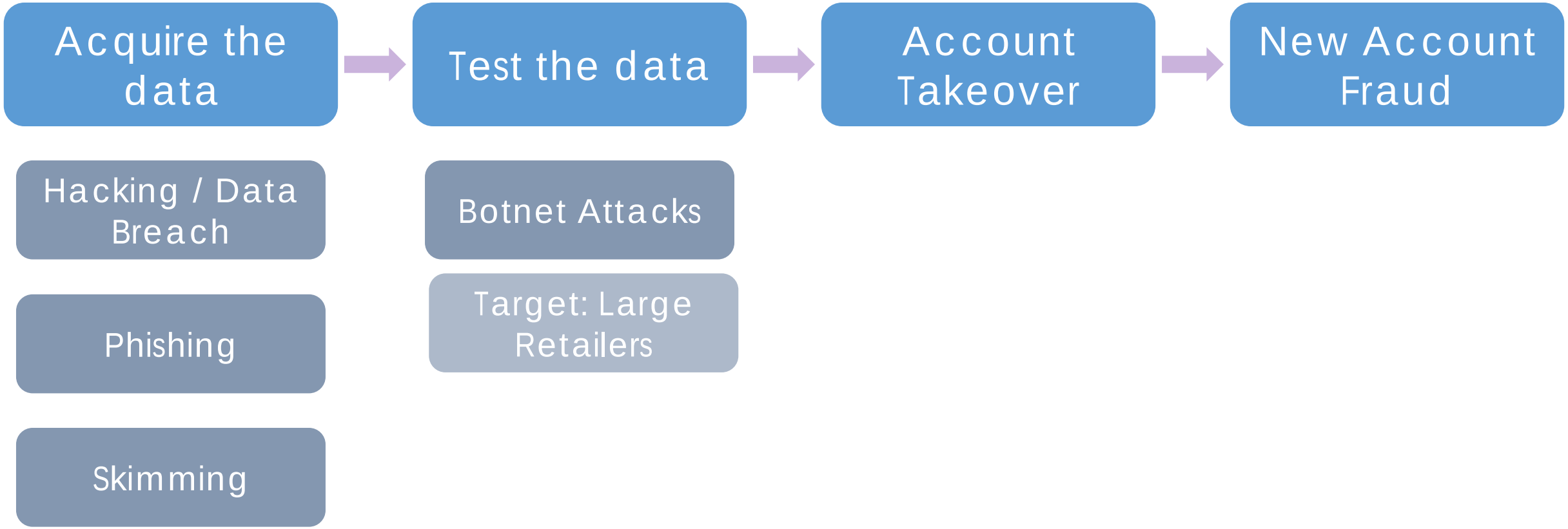
Lifecycle of CNP Fraud



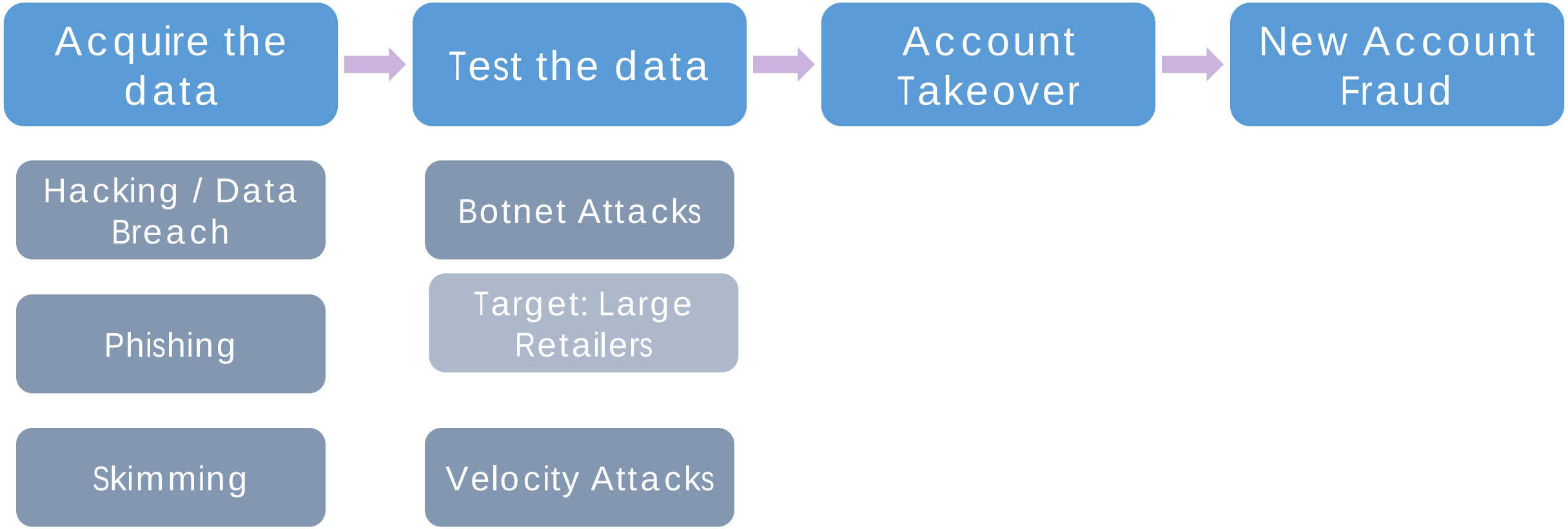
Lifecycle of CNP Fraud



Lifecycle of CNP Fraud

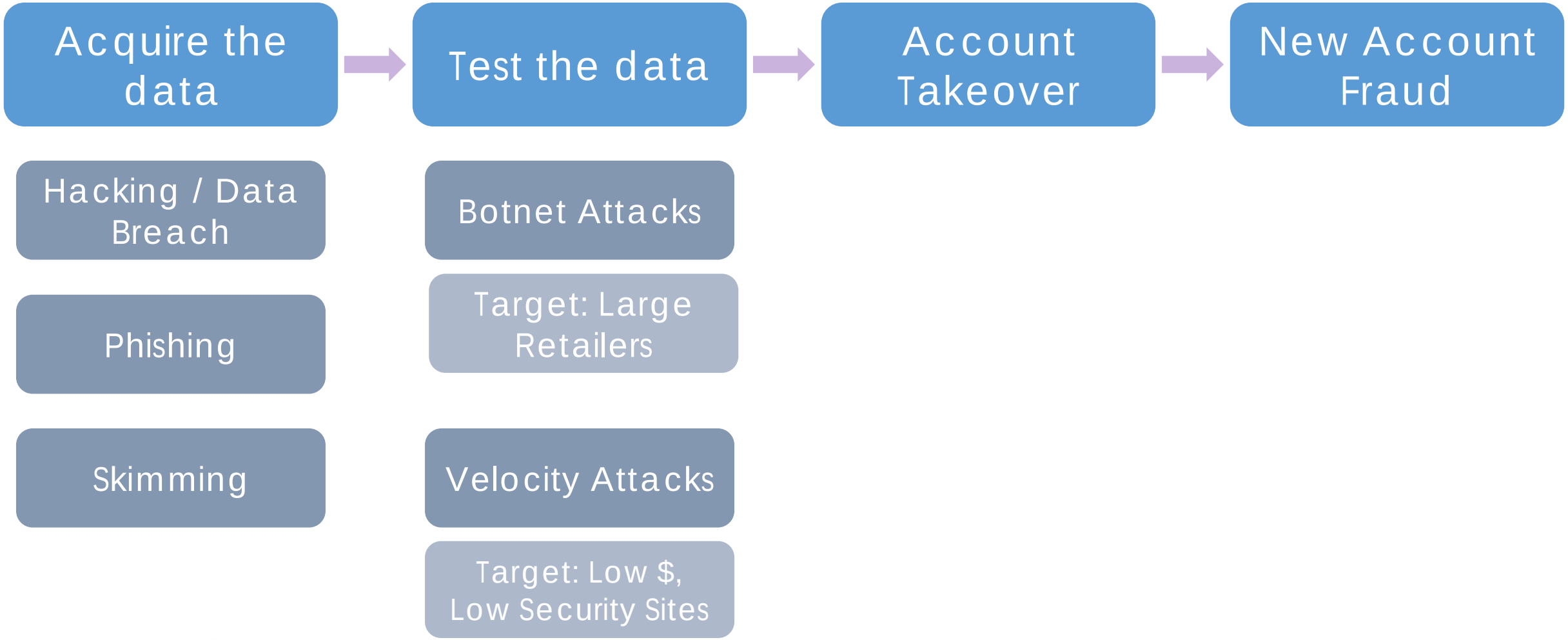


Lifecycle of CNP Fraud



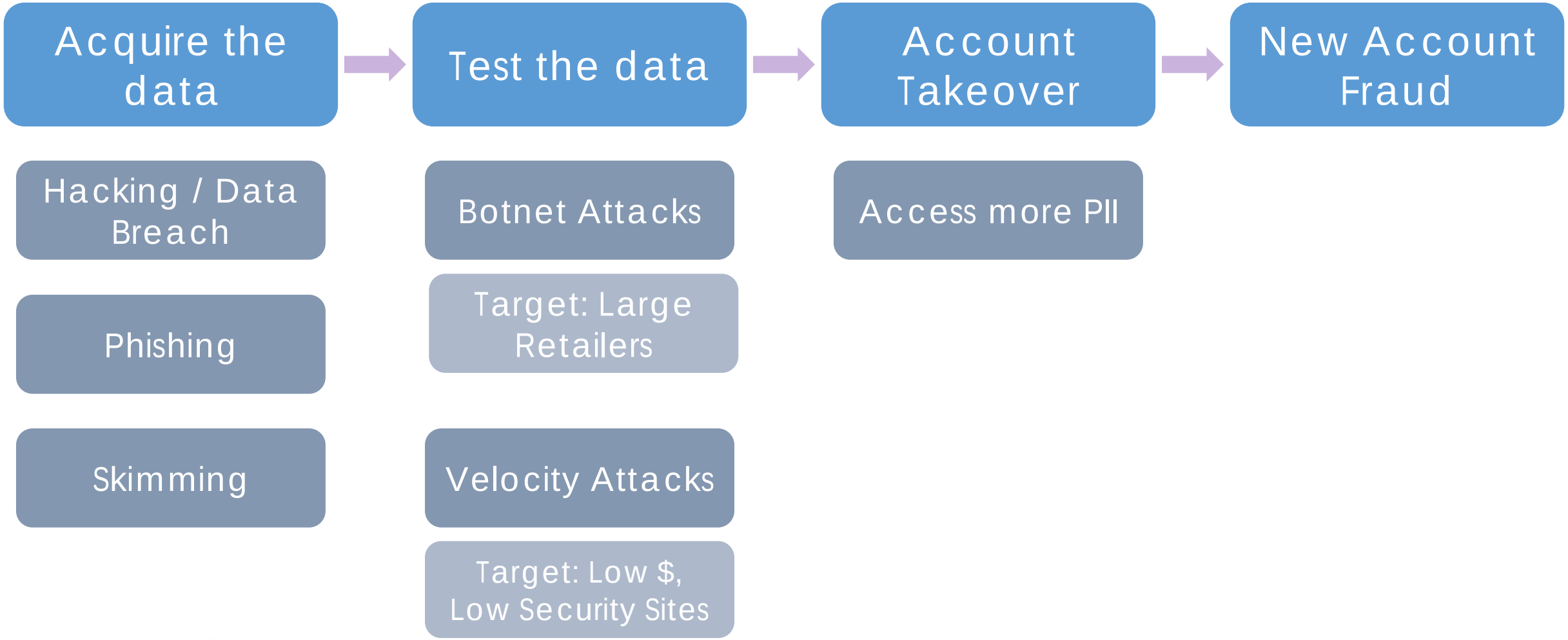
PaymentsEd FORUM

Lifecycle of CNP Fraud



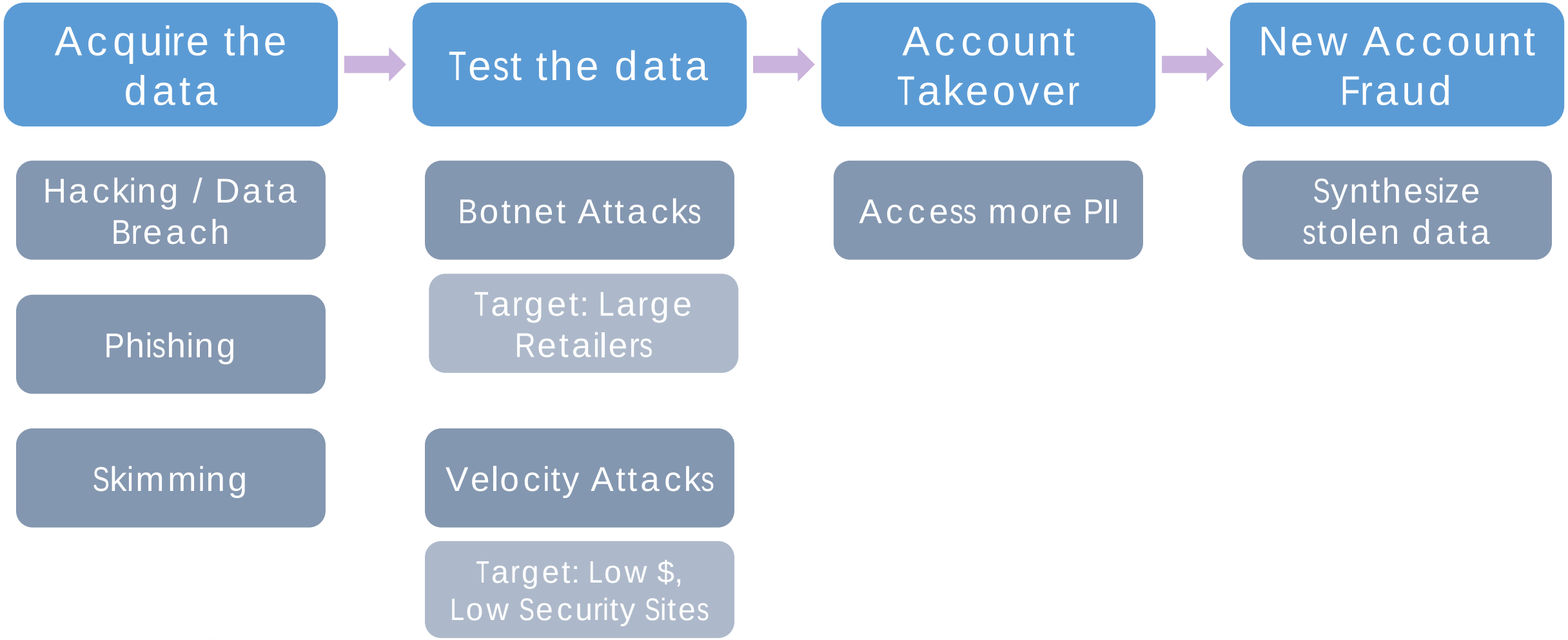
PaymentsEd FORUM

Lifecycle of CNP Fraud



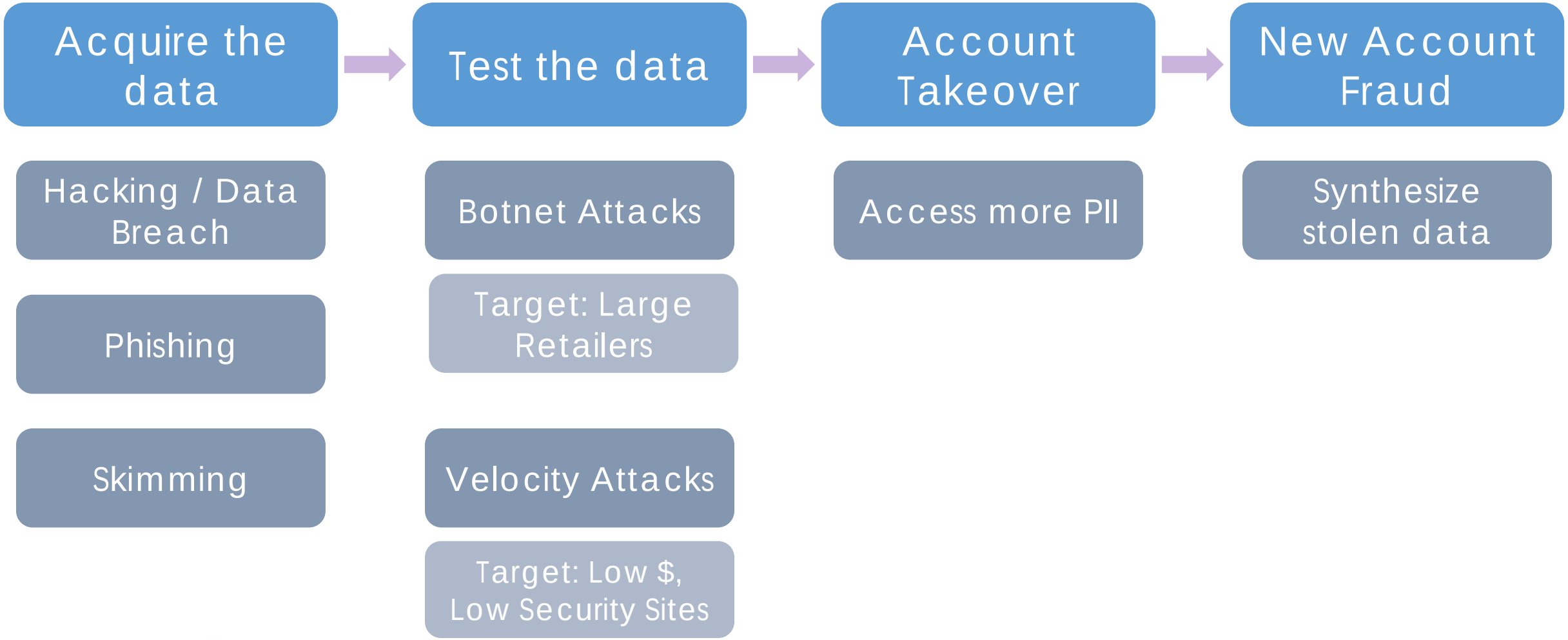
PaymentsEd FORUM

Lifecycle of CNP Fraud



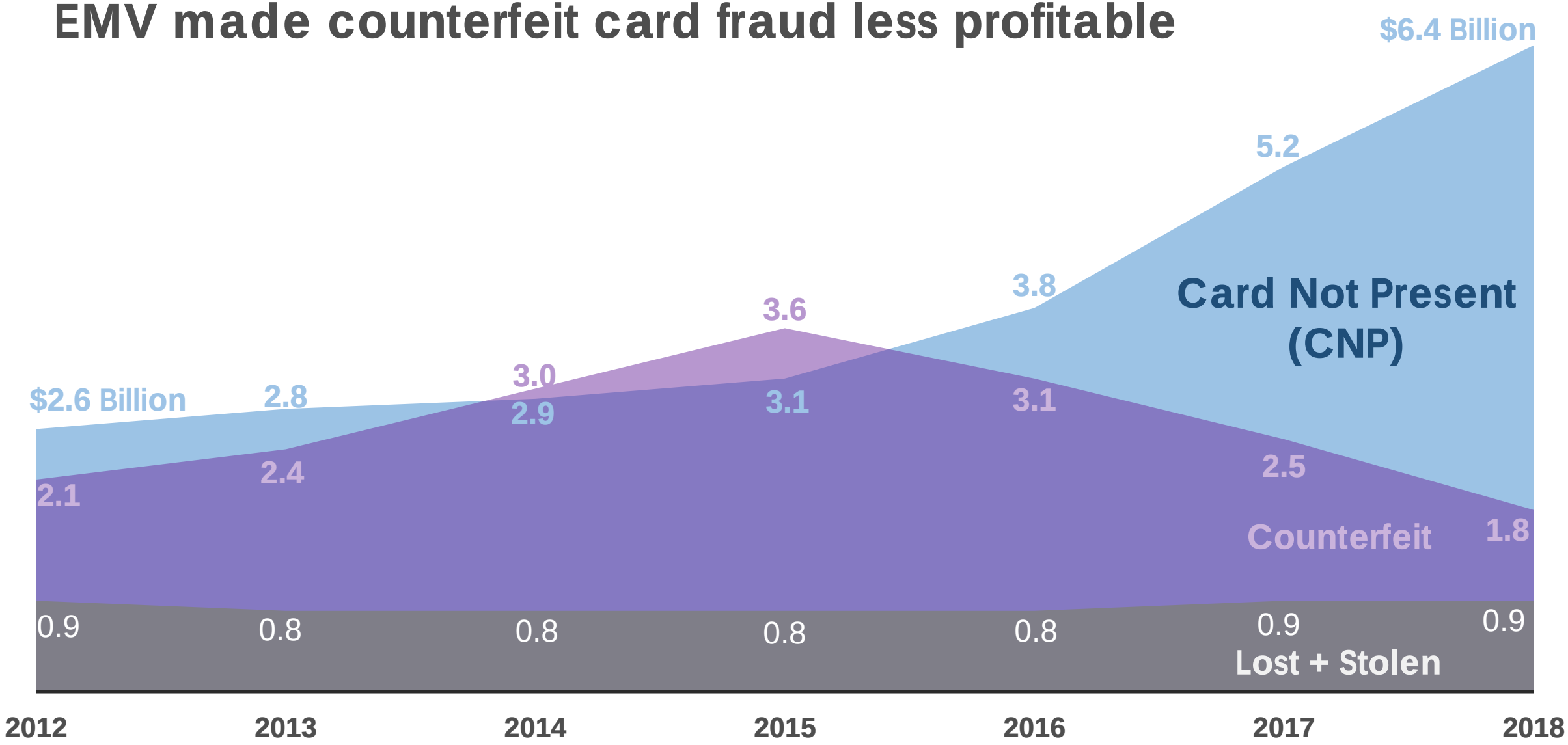
PaymentsEd FORUM

Lifecycle of CNP Fraud



PaymentsEd FORUM

EMV made counterfeit card fraud less profitable



PaymentsEd FORUM

Data from Aite Group

Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?

Counterfeit

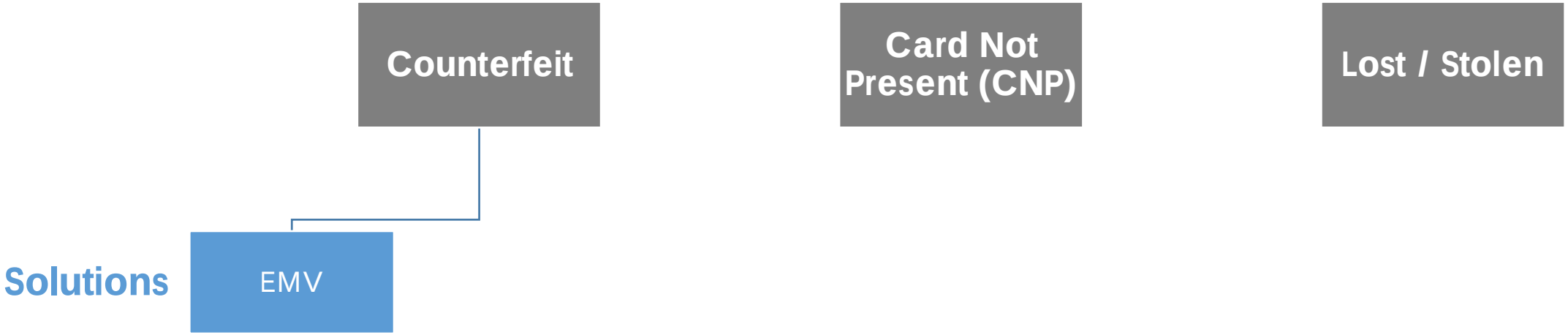
Card Not Present (CNP)

Lost / Stolen

Solutions

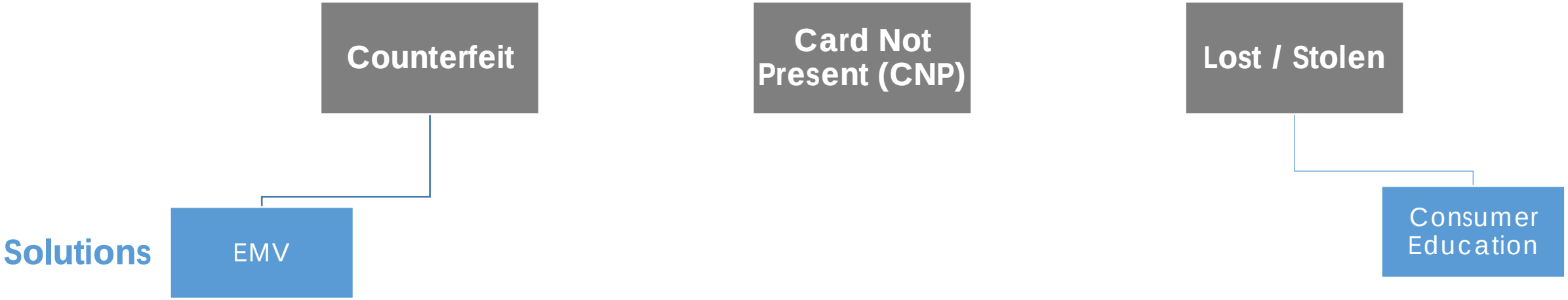
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



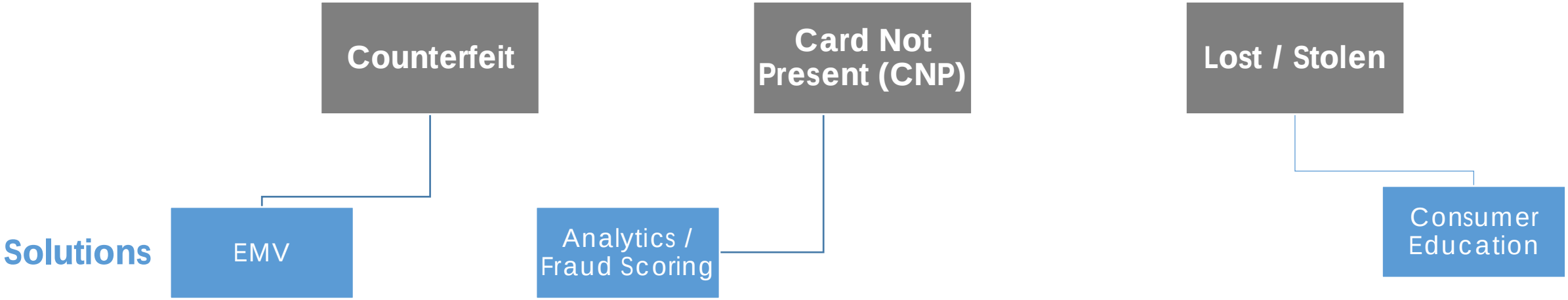
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



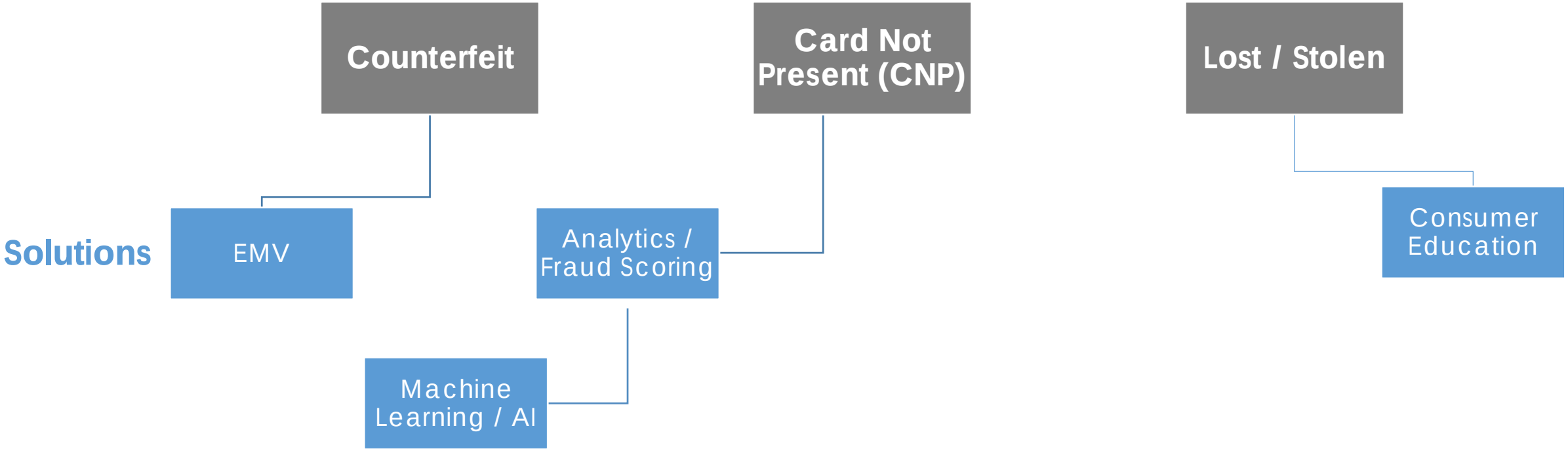
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



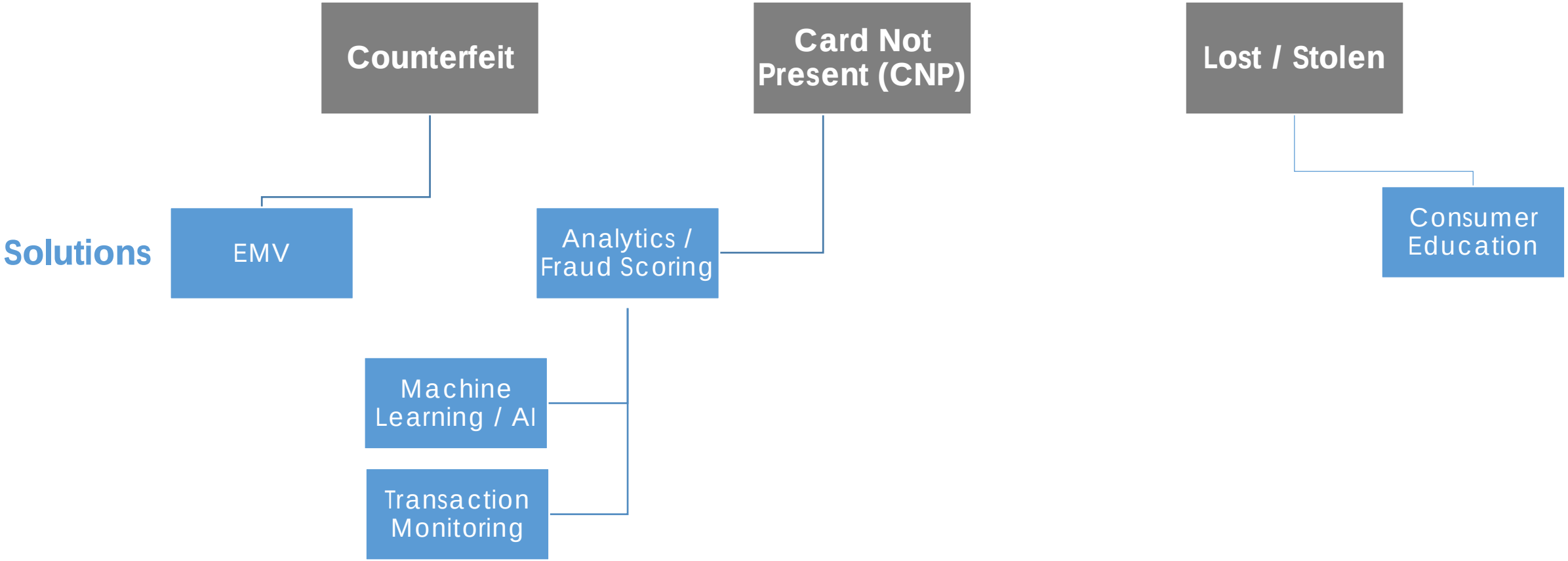
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



Fraud Risk in the Payments System

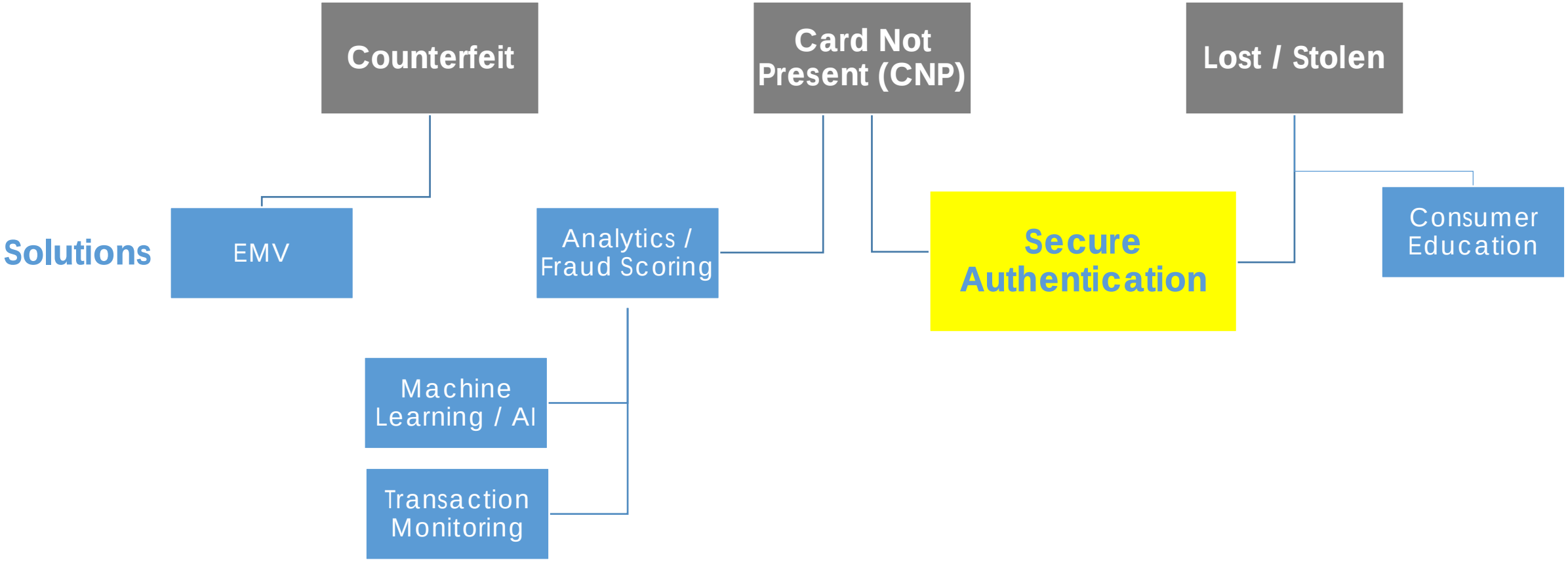
Challenge: how do you prevent criminals from using cards that don't belong to them?



PaymentsEd FORUM

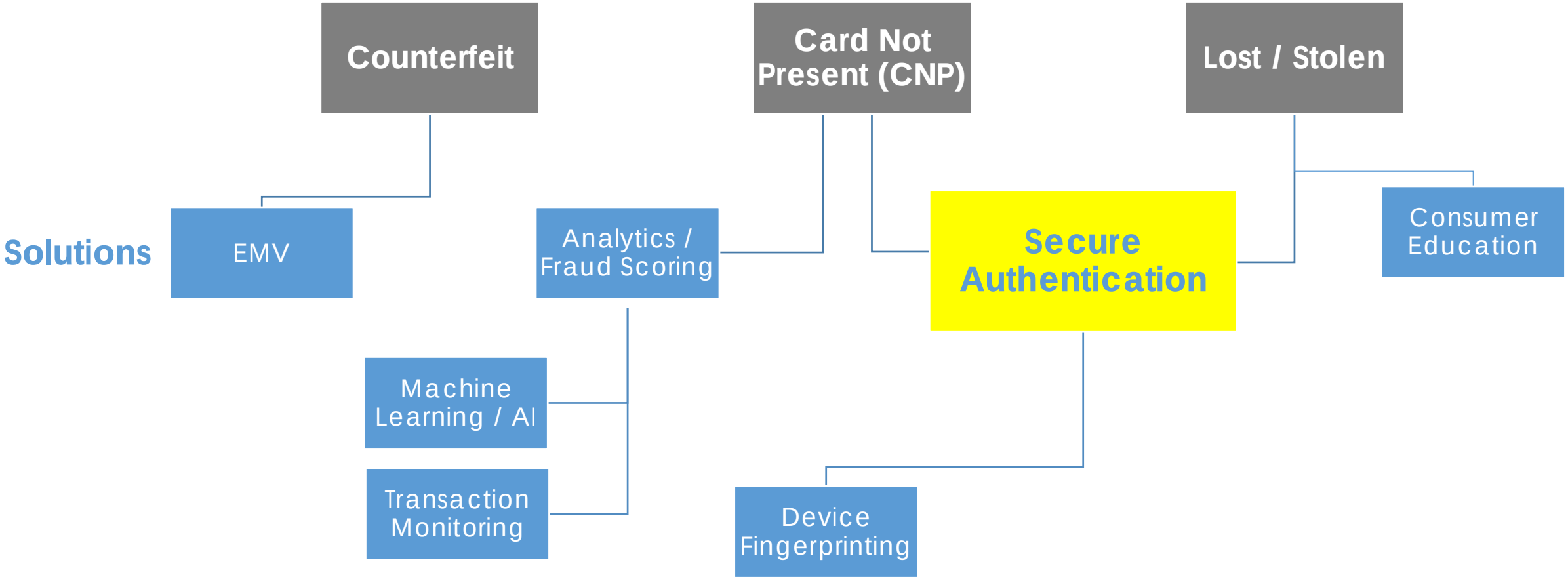
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



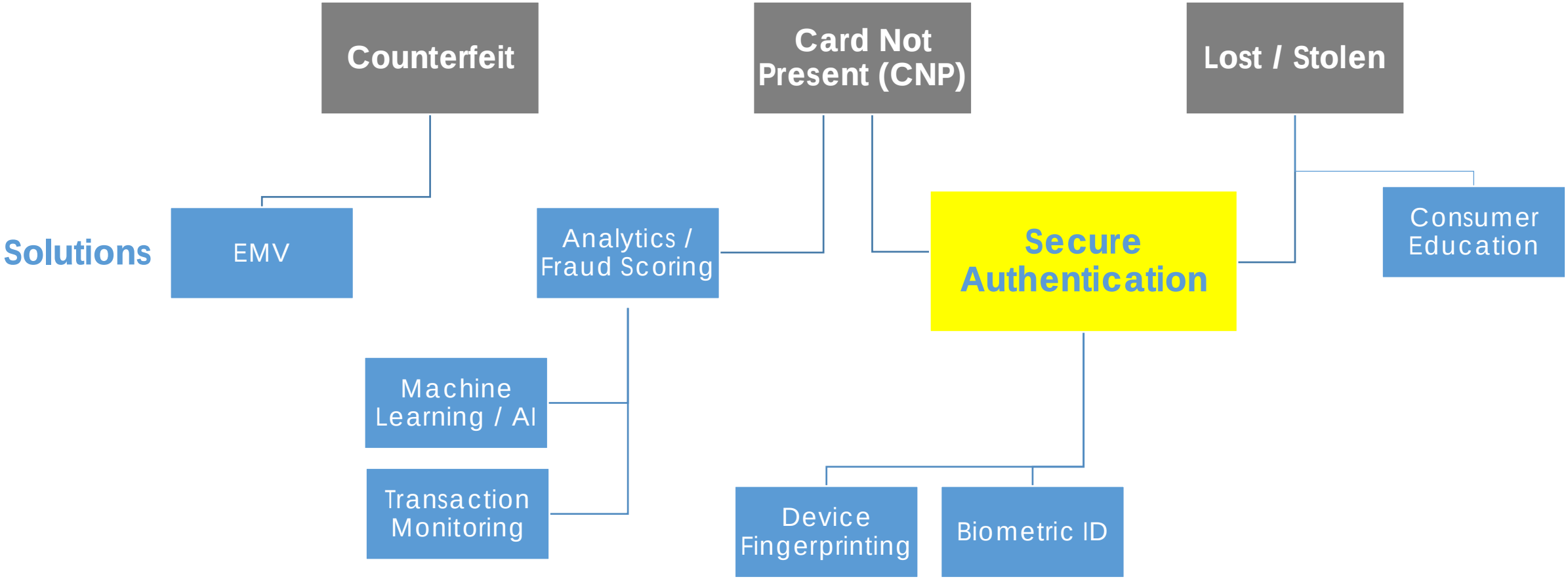
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



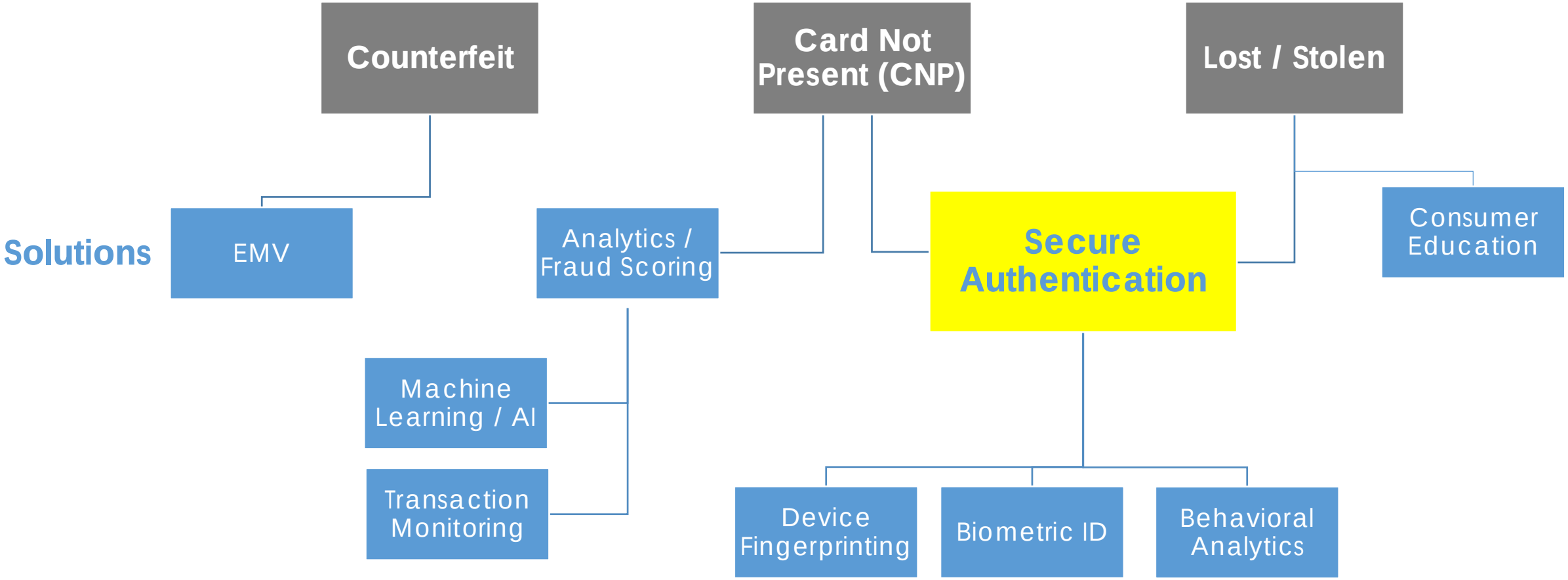
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



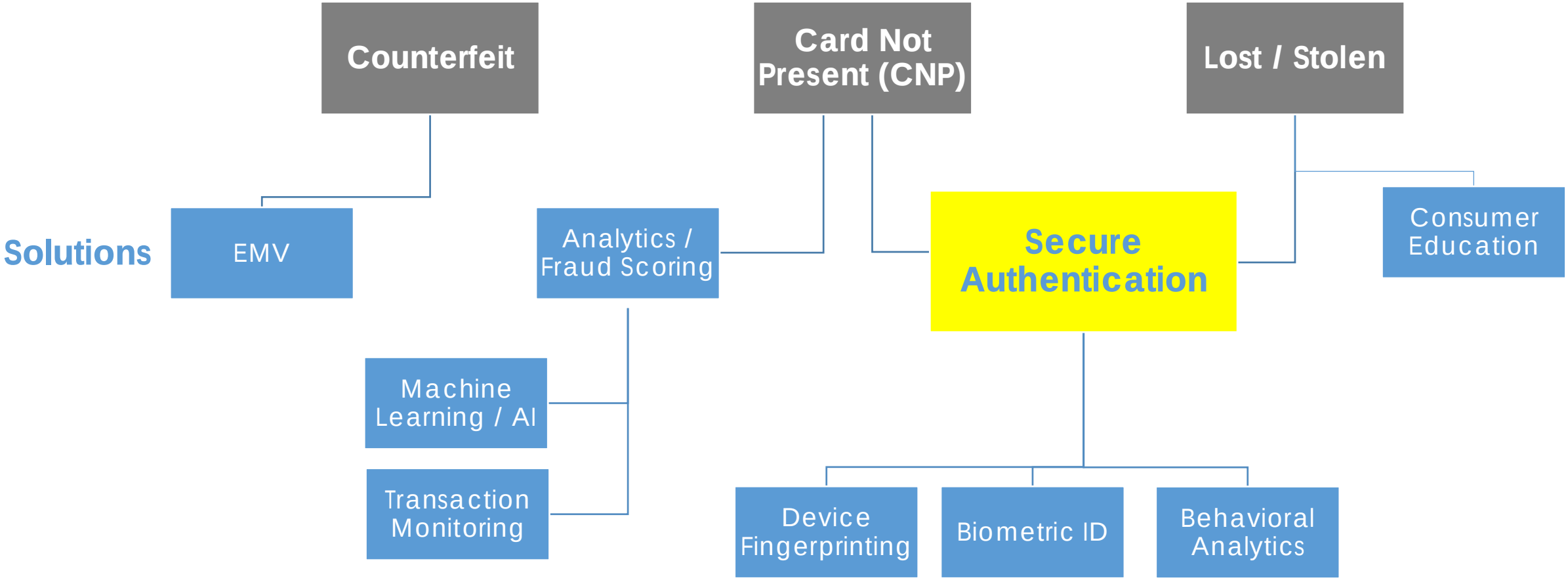
Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



Fraud Risk in the Payments System

Challenge: how do you prevent criminals from using cards that don't belong to them?



Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

One-time tokens, codes, or passwords (OTP)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

One-time tokens, codes, or passwords (OTP)

Security Questions (Knowledge-Based Authentication or KBA)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

One-time tokens, codes, or passwords (OTP)

Passwords

Security Questions (Knowledge-Based Authentication or KBA)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

One-time tokens, codes, or passwords (OTP)

Passwords

Fingerprint or iris scanning (biometrics)

Security Questions (Knowledge-Based Authentication or KBA)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

Passive / happens in the background

One-time tokens, codes, or passwords (OTP)

Passwords

Fingerprint or iris scanning (biometrics)

Security Questions (Knowledge-Based Authentication or KBA)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

Passive / happens in the background

One-time tokens, codes, or passwords (OTP)

Passwords

Fingerprint or iris scanning (biometrics)

Voice recognition

Security Questions (Knowledge-Based Authentication or KBA)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

Passive / happens in the background

One-time tokens, codes, or passwords (OTP)

Passwords

Fingerprint or iris scanning (biometrics)

Voice recognition

Security Questions (Knowledge-Based Authentication or KBA)

Behavioral analytics (i.e. keystrokes, typing speed)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

Passive / happens in the background

One-time tokens, codes, or passwords (OTP)

Passwords

Security Questions (Knowledge-Based Authentication or KBA)

Fingerprint or iris scanning (biometrics)

Voice recognition

Device fingerprinting

Behavioral analytics (i.e. keystrokes, typing speed)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

Passive / happens in the background

One-time tokens, codes, or passwords (OTP)

Passwords

Security Questions (Knowledge-Based Authentication or KBA)

Fingerprint or iris scanning (biometrics)

Voice recognition

Device fingerprinting

Geolocation

Behavioral analytics (i.e. keystrokes, typing speed)

PaymentsEd FORUM

Friction: Active vs. Passive Authentication

Most active / labor-intensive on the user's part

Passive / happens in the background

One-time tokens, codes, or passwords (OTP)

Passwords

Security Questions (Knowledge-Based Authentication or KBA)

Fingerprint or iris scanning (biometrics)

Voice recognition

Device fingerprinting

Geolocation

Behavioral analytics (i.e. keystrokes, typing speed)

PaymentsEd FORUM

MULTIFACTOR AUTHENTICATION


MULTIFACTOR AUTHENTICATION
Passwords
Knowledge-Based Authentication
Something you know


Time zone
Something you have
Geolocation
Device fingerprinting
MULTIFACTOR AUTHENTICATION
One-Time Codes
Passwords
Knowledge-Based Authentication
Something you know


Time zone
Behavioral Analytics
Something you have
Geolocation
Voice Recognition
Iris Scanning
Something you are
Facial Recognition
Device fingerprinting
MULTIFACTOR AUTHENTICATION
One-Time Codes
Fingerprint Scanning
Passwords
Knowledge-Based Authentication
Something you know


Time zone
Behavioral Analytics
Something you have
Geolocation
Voice Recognition
Iris Scanning
Something you are
Facial Recognition
Device fingerprinting
MULTIFACTOR AUTHENTICATION
One-Time Codes
Fingerprint Scanning
Passwords
Knowledge-Based Authentication
Something you know

Enhanced Authentication: 3D Secure

10x as much transaction data
+
Risk assessment

ISSUER

High-risk → require additional customer verification

MERCHANT

PaymentsEd FORUM

Thank you

- Don’t forget to submit your session evaluation!

Amy Zirkle, VP Industry Affairs
Electronic Transactions Association
@ElecTranAssoc
electran.org