The State of Play in Cyber Payments Fraud

Improving Security for Online & Card Not Present Transactions

Mark Greene, Ph.D
CEO, FICO

Federal Reserve Bank of Chicago
26 September 2011

Cybercrime Costs

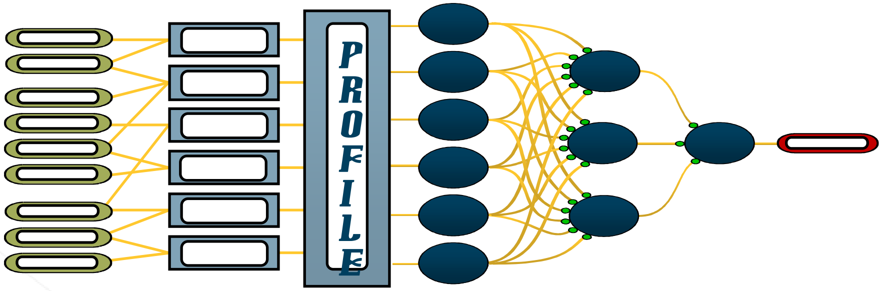
- 431 M adult victims globally in the past year
- Annual price is $388 B globally (financial losses + lost time)
- Cybercrime costs the world more than the combined global black market for marijuana, cocaine, and heroin ($288 B)
- 69% of online adults have been a victim of cybercrime during their lifetimes
- 10% of adults have experienced cybercrime on mobile phones
- Only 16% of adults who access the internet from mobile devices have up to date mobile security

Source: The Norton Cyber Crime Report 2011

Merchant CNP Fraud Detection:
Online Fraud Management Trends and Issues

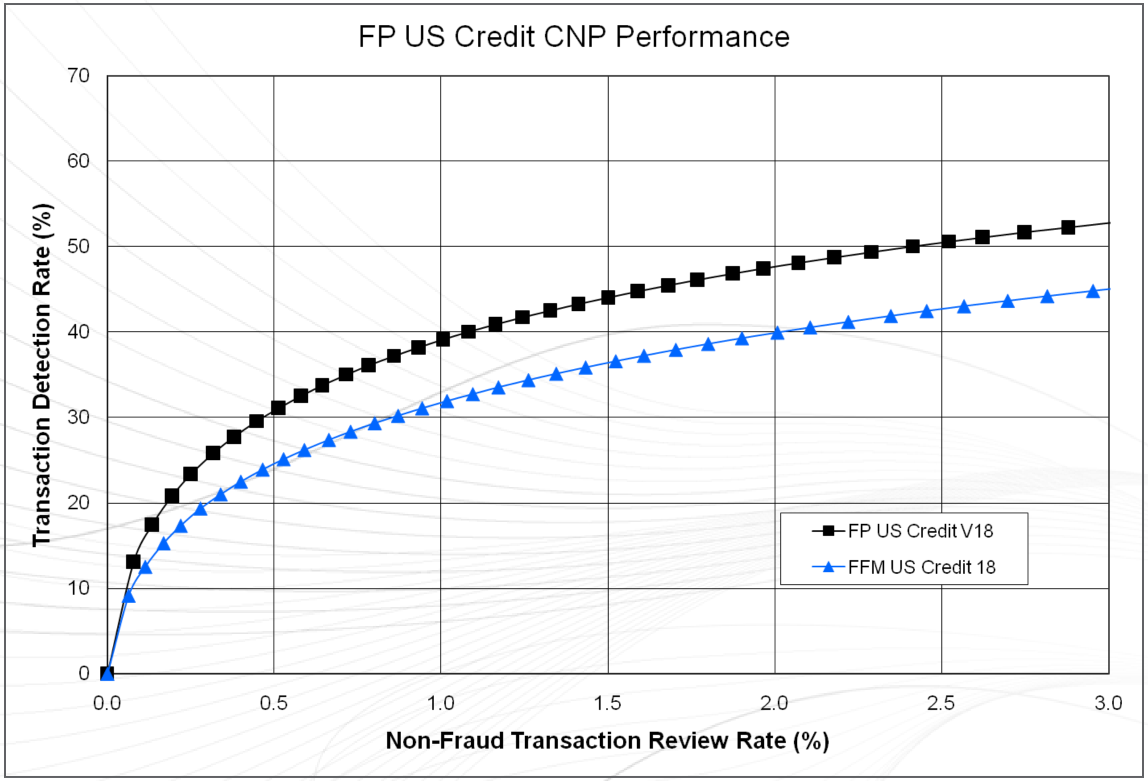
- Incidence of card-not-present (CNP) fraud is much higher than in-person / POS shopping fraud… Why?
  - CNP transactions are lower risk / lower effort for fraudsters
  - Issuers generally don’t carry the loss risk
  - Merchants are (understandably) focused on sales
- Online/CNP fraud is expensive
  - Higher order volumes mean higher losses
  - Blocked orders decrease revenue
  - Retailers lose payments, cost of goods, shipping charges and eventually credit card privileges
- Fraud must be detected in relevant time
  - Stop fraudulent transaction before delivering goods or service
  - Real time fraud management systems are a must

Merchant CNP fraud detection:
Use merchant profiles + traditional cardholder monitoring



- Standard neural network approaches only leverage cardholder profiles
- Merchant profiles give neural networks the power to compare historical merchant activity with recent order patterns
- Merchant profiles close the feedback loop
  - If fraud occurs at a merchant, the merchant’s account (usually) stays open
  - Fraud information is added to merchant’s profile
  - Fraud on one card informs future fraud risk on another card
  - Significant improvement over standard cardholder profiling
  - Note: not fraud committed *by* merchant; fraud committed *at* merchant
- Merchant profiles are dynamic
  - Industry view: Updated weekly based on latest activity, including confirmed frauds
  - FI view: Global intelligent profiles (patented)

Merchant CNP fraud detection: FICO Falcon Fraud Predictor with Merchant Profiles



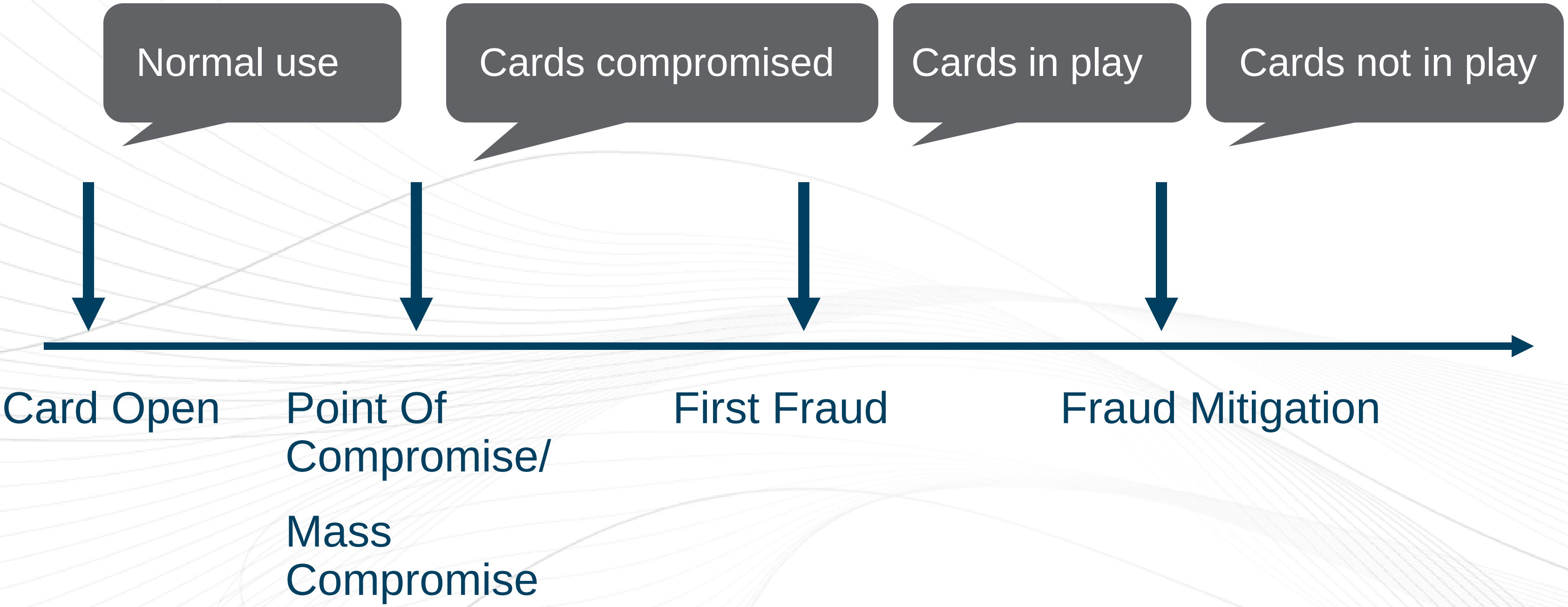
FICO Falcon Fraud Predictor profiles monitor all aspects of merchant behavior including:

- Card Present and Not Present
- Domestic and Cross-border
- POS Entry – Keyed, Swiped, Chip

- Provides improved card-present / card-not-present distinction and variables
- ~33% relative lift in incidence detection at a 0.5% review rate

Mass Compromise: Fraudulent Card Life Cycle

Timeline



Normal use

Cards compromised

Cards in play

Cards not in play

Card Open

Point Of Compromise/

Mass Compromise

First Fraud

Fraud Mitigation

Compromised cards are gradually released to black market

Make better decisions by knowing a card is compromised

Mass Compromise: Detection

- Identify mass compromise at merchants
  - Where: Which merchant sites are compromised
  - When: When the compromised occurred and the extent
  - Who: Which cards are compromised
- Identify suspicious test sites & tested cards
- Create Compromise Clusters
  - Monitor
    - What clusters are hot and active?
    - Where is CNP and testing behavior occurring
  - Rank: Order cards in the compromise by a compromise card score

Working with Law Enforcement – Success Story

- Leveraging our Card Alert PIN-debit fraud system, FICO recently aided law enforcement crack a coordinated ATM compromise of cards & PINs (aka… the ‘Big NY Case’)
  - FICO alerted US Secret Service to compromises and resulting fraud
  - Having an industry view of the problem, FICO provided impacted financial institution contacts to law enforcement to work losses more efficiently and build case
  - FICO provided **link analysis** of fraudulent activity across banks, and fraud reports predicting where the criminals might hit next
  - FICO was subpoenaed for evidence used in convictions of suspects
- FICO also worked with ATM networks to establish ‘rooster’ alerts
  - When criminals use cards identified as ‘at risk’, pager alerts USSS to physical address of ATM in real time
  - Several arrests made

Lessons Learned Working with Law Enforcement

- Previously *established* relationships with organizations and sharing of critical information lead to successful outcomes (i.e. don't wait for a problem to initiate the relationship)
- If the law enforcement agency does not view organization as the entity experiencing losses, often they do not want to share or request assistance
- Loss amount thresholds will come into play, particularly in large cities, which require industry shared fraud information to meet thresholds – can't do it alone
- Leverage experience with one agency to get make contact with another agency in different region, etc…
- Provide subpoena information as quickly as possible, discuss format and information with the agency ahead of subpoena
- Collaborate; but be certain to protect your proprietary secrets in subpoena responses
- Agencies have multiple duties and other cases may take precedence (e.g. election duties come first for USSS in election years)