Modeling Credit Card Fraud

Michael Alliston

NUMERACY, LLC
VALUE BEYOND THE NUMBERS

NY INFORMS Chapter
October 16, 2002

What we will cover today . . .

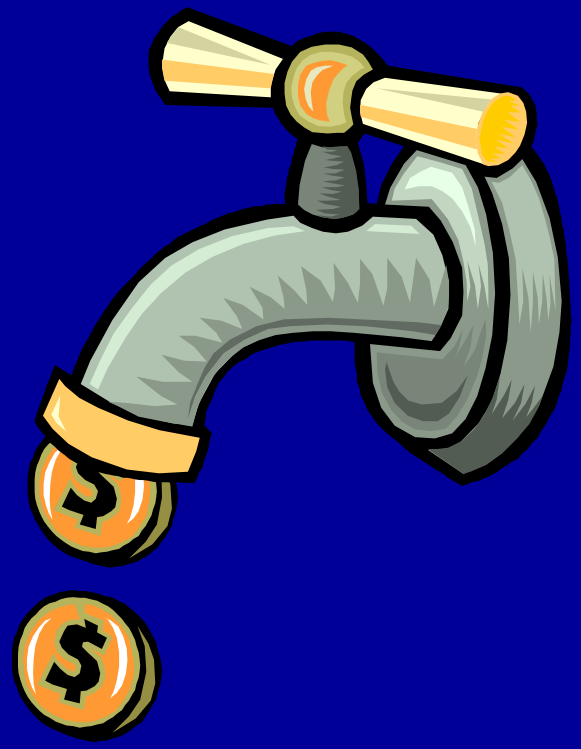
- Fraud as a payment industry problem
  - How Payments and Fraud work
  - Consequences for modeling
- Common general purpose transaction models
  - Business drivers, pros and cons
- Newer problem specific models
  - “Skimming”
  - “Bust outs”

Fraud is a Big Small Problem

Total Annual credit card losses across major brands approach
$2 Billion

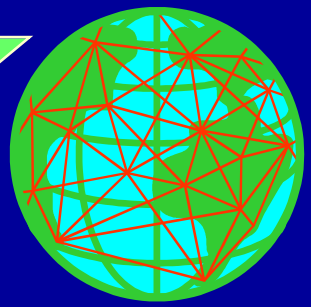
. . . But this is only

Roughly 8 basis points of all transaction volume



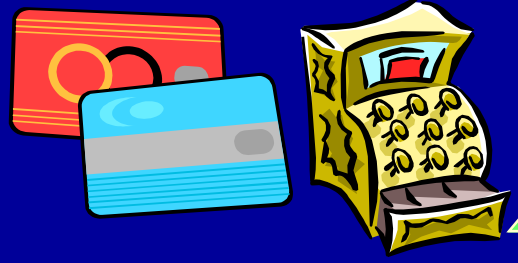
Credit Card Players

An **Issuer** bank issues you a card, sets rates, bills



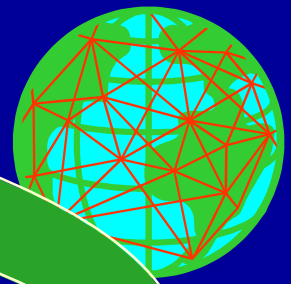
Card Companies provide

- Telecommunications
- Settlement
- Rules
- Administration
- Security



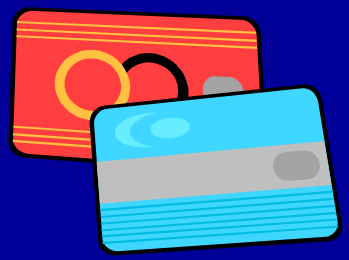
An **Acquirer** bank sets up merchants

Authorization Transactions



Response

Message path: Merchant, Acquirer, Association, Issuer and back in seconds



Request

Rules of the Game

- Card Associations “never” deal directly with cardholders or merchants
  - These relationships belong to the issuers and acquirers
- Card Associations have NO personal cardholder information - only account numbers
- Fraud losses are losses to the Issuer, except that . . .
- The Merchant takes the loss if
  - Merchant fails to follow procedure
  - Card not present
  - Merchant has “excessive” fraud

Industry Behaviors

- Fighting Fraud is a business issue, not a moral crusade
  - All players weigh ***their*** cost /benefits of fraud prevention
- Card Companies fight fraud to protect
  - Brand image and overall consumer confidence in card use
  - Competitive advantages to issuing / accepting their brand
- Players compete and do not readily share information
- Obsession with service levels, consistency, planning
- High systems requirement for coordination among players

Consequently, change is slow

So what is Fraud?

Any attempt to steal by defeating one or more of

- Card Features
- Authorization process
- Merchant procedures or practices
- Acquirer procedures or practices
- Issuer procedures or practices

Fraud happens many ways . . .

- **Lost or Stolen**
- **Never Received** - Card intercepted without reaching the account owner
- **Fraudulent Application** - Card acquired by falsifying a credit application
- **Multiple Imprint** - Same card used multiple times
- **Account takeover** – Criminals effect address changes on valid accounts, receive new cards, and in effect take control of the account

And. . .

Some more ways . . .

- **Counterfeit** - Unauthorized plastic made or altered to appear to be a legitimately issued card
- **Card Not Present** - Mail /Telephone/ Internet
- **Account Generation** – Creation of possibly valid account numbers and expiration dates for counterfeit or card not present transactions
- **Familiar Fraud** - Cardholder claims fraud to protect a "close" person
- **Credit Abuse** - Typically not treated as fraud, but as a collection problem
- ***Etc.....***

Consequences for Modeling

- Different fraud schemes require different models
  - General purpose transaction models often use subordinate models for specific fraud conditions
    - Rules based systems
    - Neural networks with special features
- Masses of transaction data require high efficiency
- Databases of fraud history exist, but
  - Fraud is reported slowly - 30 to 90 days after the event
  - Are transaction based and miss relationships among events
  - Data is incomplete and very dirty
  - Fraud definitions are not MECE, type is often not really known
  - Codes and structure respond very slowly to new fraud schemes

Major Industry Focus has been on General Purpose Transaction Models

Object: Detect fraud *transactions* in "near real" time

- Rules based "expert" systems
- Neural Networks
  - Profiles of Cardholders and Merchants
- Hybrid of the above
  - Rules to screen for real time scoring by Neural nets
  - Neural Net Scores fed to rules
  - Rules for combining multiple Neural Net scores

False Positive and Detection Rates drive everything

Economic Issues for Transaction Models

- Fraud Detection Rate leads mysteriously to fraud savings
  - Typical 25% to 50% claim
  - What exactly is saved?
    - Average loss per fraud account may be only a few hundred dollars
    - Open to buy – the credit left
    - How many fraud transactions does it take to get an alert?
    - What did the bank do with the alerts?
- False Positive Rate translates directly into operating costs
  - Typical 9:1 to 30:1 - some at 5:1 and 100:1
  - Every positive consumes human resources in phone calls, letters, account actions

Economic Issues for Transaction Models

- Real time intervention is extremely expensive, and has a big risk of negative customer reaction
  - Embarrassment in a store becomes a favorite story
  - Choosing another card
  - Merchant asking shoppers for a different card
- Near real time detection delays intervention, but avoids most negative reaction
  - But there is a current trend to more aggressive intervention without customer contact

Pros and Cons of Neural Nets and Rule Models

	Neural Nets	Rules
Pros	• Transcend Your experience • Persistent good performance • Supports individual profiles	• Easy to understand • Explainable • Easily modified • High control • Cheap, quick
Cons	• Some unexplainable results • Long time to retrain • No control • Costly	• Reflects limited experience • Good performance requires constant tweaking • Interaction among rules hard to untangle

Recent Shift to Special Purpose Models

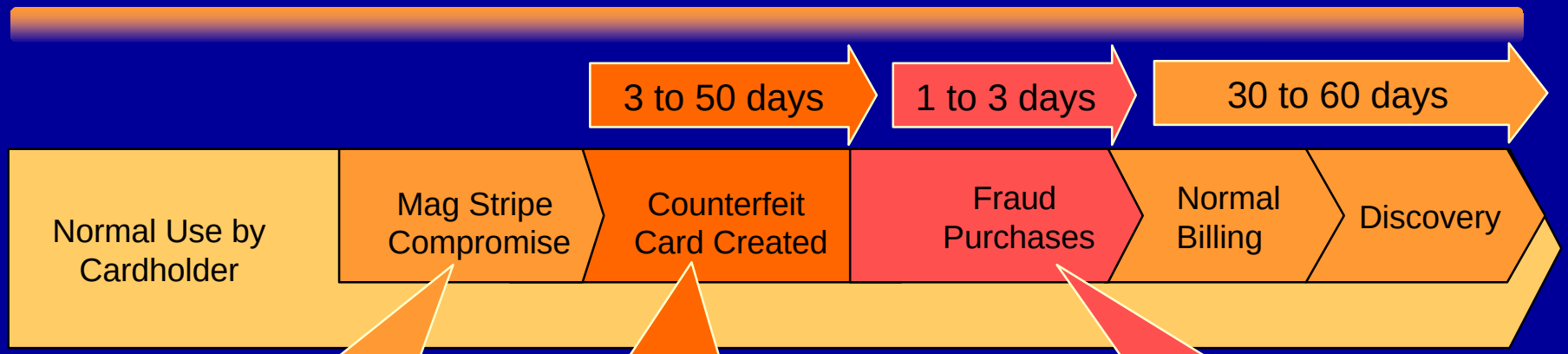
Object: Detect *specific* fraud *patterns* in "effective" time

- Models for the Merchant's use include click-stream and other data not available to institutions or associations
  - Purchases grouped by address or phone instead of account
  - Underlying neural nets, rules, or both
- Heuristic Models are good for specific fraud types
  - Skimming
  - Bust outs

New Modeling Environment

- Little or no history data - these models address patterns involving more than one transaction
- Requires building a consortium of interested parties willing to share information
  - Only recent data is available
  - Much is anecdotal
  - But, anecdotes reveal what to look for
- Improvement through iterations of user review and model development
- Early wins generate more active consortium interest
  - More data and more insight

Skimming



- No Fraud on this purchase
- Is it a crime?
- Merchant location is a point of compromise
- Typically takes your card out of sight and has high employee turnover

- Compromised numbers may be used locally or sold to large organizations overseas
- Counterfeit cards with perfect mag stripes are sold to criminals in packs of 50 to 100
- Is this a crime?

- Fraudster uses card a only a few times
- Never knows how much credit is left
- Location be unrelated to cardholder

Defeats all card and process checks
Largest growing threat in recent years

Detecting Skimming: Concept

- Object is to identify the Point of Compromise and shut down the source of the card data to counterfeiters
- For all “current” counterfeit fraud transactions, gather **all** transactions for a common prior period, sort by merchant, and flag these as pre-fraud
- By merchant, calculate the percentage

$$\frac{\text{Pre-fraud accounts seen at that merchant}}{\text{All accounts seen at that merchant}}$$

- Some tweaks and twists apply

Detecting Skimming: Results

- Points of Compromise stick out noticeably
  - False positive rate of 5:1 easily achieved
  - Attempts by individual institutions and smaller consortia get nowhere near these results
  - Large card companies are uniquely positioned to do this kind of analysis because of the wealth of transaction data
- Secondary results assist investigations: Cards with a common POC
  - are often used at a small “ring” of merchants
  - have a tight range of time between compromise and the first fraud

Cardholder Bustout

- A Bustout occurs when a cardholder rapidly spends a set of cards to the limit, pays with bad checks to restore the credit line, spends it all again, and disappears
- An extreme form of deliberate credit abuse
  - Cards are with the real cardholders
  - Cardholder collects a “wallet” of cards
    - May be new, or “nurtured” to achieve high credit limits
  - Easy to run up $100,000 plus over several banks
- Typical pattern is heavy use of new or previously low-activity accounts

Merchant Bustout

- Cardholder Bustouts focus on high ticket items easily converted to cash
- Some merchants collude in this
  - Merchant may be the cardholder
  - Merchant may be only an account and no merchandise is involved at all
- Typical pattern: All transactions are with a few merchants, and a few transactions on each card
  - Usually more cards than merchants
  - Chains of transactions and accounts link merchants

Detecting Bustouts

- Filter for heavy use of new and recently low-activity accounts
- Use these to select merchants with a high percentage of sales from these accounts
- Group merchants by activity on these accounts
  - Some eliminations and tweaks apply
- Results in groups of merchants and to some degree cards that indicate organized rings

Conclusion

Fraud detection modeling is

- Difficult and challenging technically, both from a modeling and computing perspective
- Fraught with organizational and political problems
- Rich and largely unexplored problem territory
- Immense Fun