AFP®
Annual Conference
OCTOBER 27–30, 2013 | LAS VEGAS
ORIGINAL→ESSENTIAL→UNBIASED→INFORMATION

Association for Financial Professionals®

Case Study
Responding to a Sophisticated e-Commerce Fraud Attack

Mitch Muroff
Curaxian Inc.

Denise Aptekar
oDesk

Agenda

- Introductions
- The Case (Merchant, Best Practices)
- Typical Screening Methodology
- Circumvention Methods
- The Attack
- Our Approach & Results
- Cleaner Fraud: Implications & Solutions

Curaxian

- Consulting + Analytics: We help merchants find solutions to difficult fraud problems.
- Curaxian Analytics: SaaS based reporting, monitoring, and analytics.
- Plus:
  - Reduce authorization declines to increase order conversion and billing revenue
  - Reduce interchange downgrade costs.

oDesk

- Online marketplace for remote work projects
- 4M freelancers and 400K employers
- Work project is digital good
- Most transactions are international
- Guarantee funds to the freelancer
- Clients pay after receiving deliverable

The Case

- Fortune 500 global merchant.
- Selling tickets through online web site.
- Following all standard best practices.

Order Page	CC Auth	Score	Review	Accept/ Reject

- Discovered excessive chargeback levels.
- Could not find solutions in data.
- Requested audit and deep data analysis.

Typical Screening Methodology

- Identify high velocity correlated with risk (approval/decline, count/amount, by device, card, IP, email, etc.).
- Identify high risk geographic locations or inconsistencies.
  - Location of: IP address, card issuer, billing address, phone, etc.
- Validate data provided.
  - Address, CVN, name, phone, email.
- Most merchants have similar rules; criminals develop methods that can circumvent controls across many merchants.

Methods: Valid Card Data

- Merchants check billing address and CVN but fraudsters buy stolen cards on the black market with names, billing addresses & CVN

- For United States Of America Banks

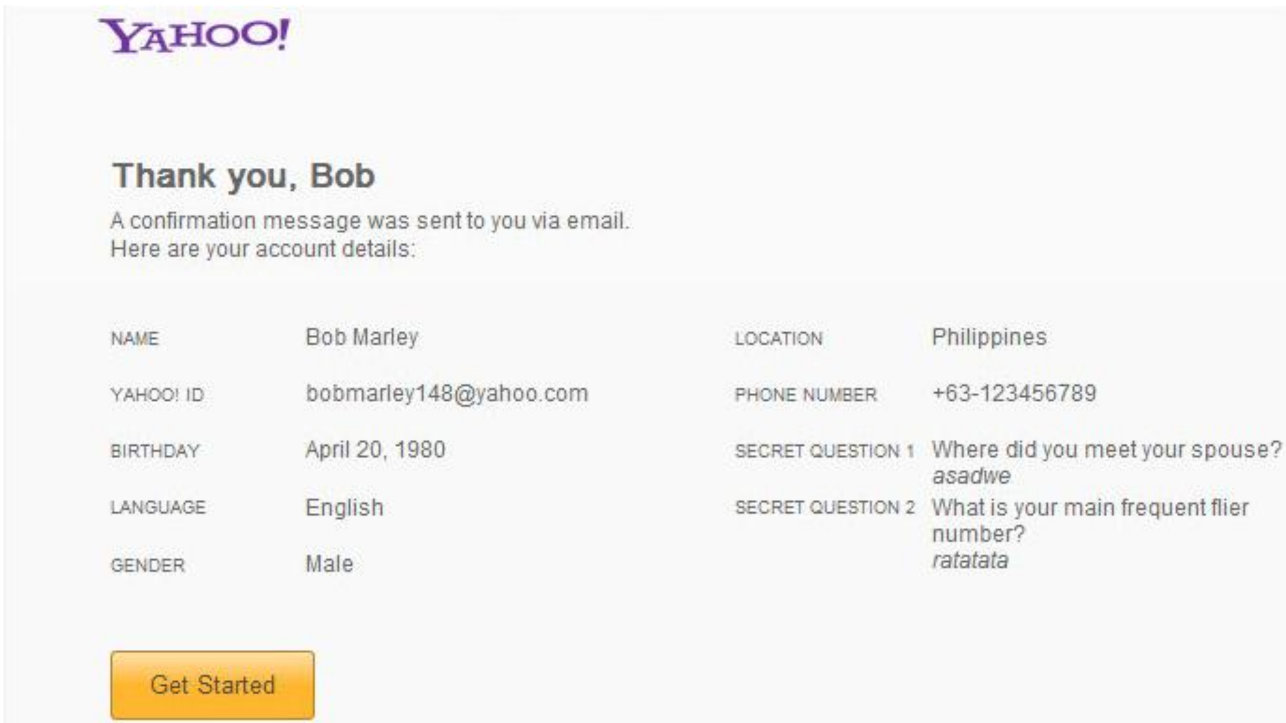
Bank Names	Balance	Price	Preview Screenshot
Bank Of America	Between 2k - 50k	400$	Download
WellsFargo	Between 4k - 40k	300$	Download
Chase Bank	Between 2k - 30k	250$	Download
Citibank	Between 9k - 70k	300$	Download
Wachovia	Between 2k - 18k	275$	Download

Methods: Valid IP Address

- Merchants check type of IP address and look for IP addresses in high risk locations or far from cardholder location but fraudsters hide their real IP location.

Methods: Valid Email Address

- Merchants may limit accounts to 1 email and check for email from high risk areas but fraudsters have access to unlimited email accounts.



Methods: Valid Phone Number

- Merchants may verify that phone is located near cardholder but fraudsters can gain access to #s in any location

Methods: Designing The Attack

- Conduct R&D on a target site
- Gain access to source of funds, identities and exit methods
- Test accounts first before conducting real fraud
- Fast exits
- Social engineering

The Attack

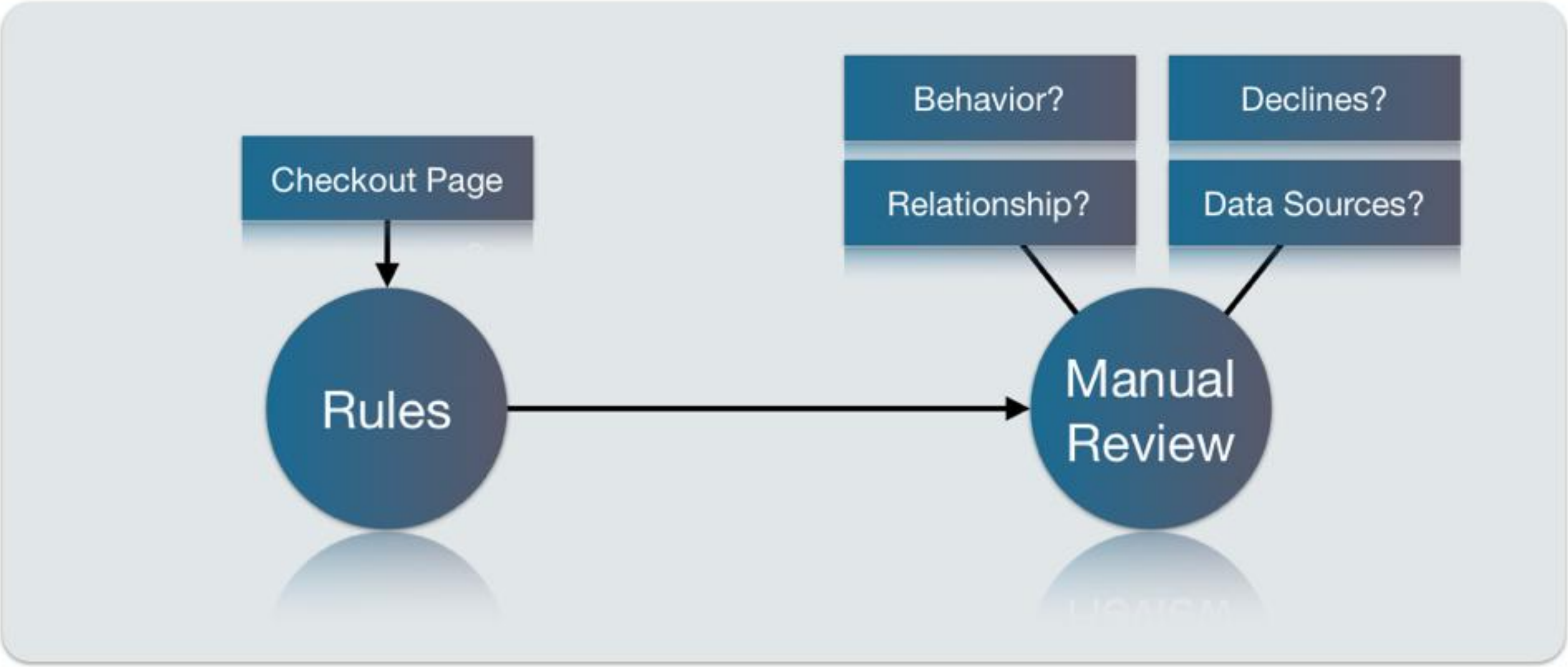
- Every order had matching AVS and CVN.
- Names and addresses appeared to be valid.
- Every order had a phone number that appeared valid.
- Nearly all fraudulent orders had free email accounts, but most good orders did as well.
- There was no velocity against card, email, or IP.
- Chargeback rates were unacceptably high.
- No obvious rules could be developed to separate good from bad orders.

Our Approach

- 400 variables.
- Which combinations of variables are best?
- Reduced to 25 variables.
- 16,000 potential solutions.
- Almost 600% difference from worst to best.

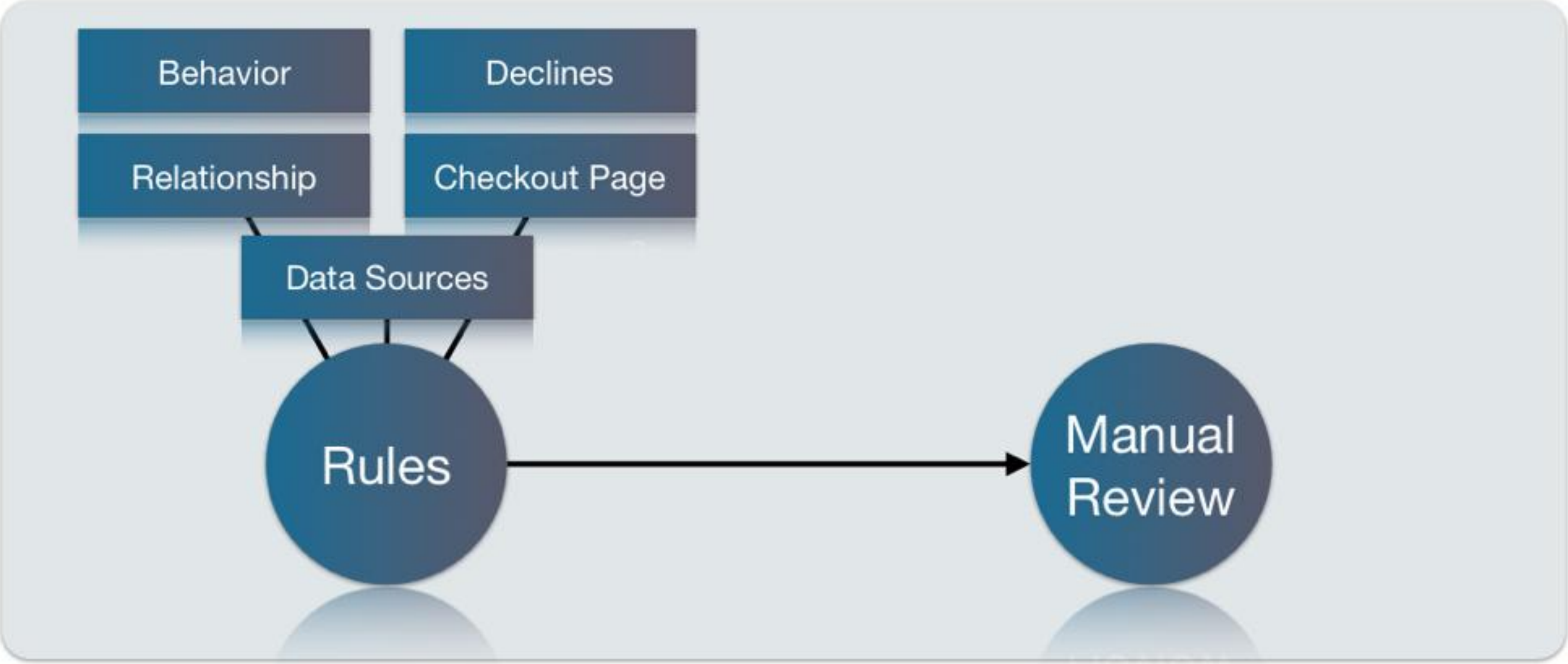
Minimal Data @ Rules = Inefficiency

Most data is cobbled together by manual labor, if available at all: Higher false positive rates and labor costs.



More Data @ Rules = Efficiency

When more data is available to rules, they can **catch more fraud at a lower cost** (false positives & manual review).



62% Fraud Reduction: 1 variable.

A

Cost	Fraud Reduction	Dimension 1	Dimension 2	Dimension 3	Dimension 4	Dimension 5
0.49	$1,320,367	IP Region Risk	Product/Service Bucket	Item Count Risk Bucket	Email Domain Risk Group	Card Brand
0.49	$1,213,563	IP Region Risk	Product/Service Bucket	Item Count Risk Bucket	Email Domain Risk Group	Order Date/Time Bucket
0.47	$1,182,253	IP Region Risk	Product/Service Bucket	Email Domain Risk Group	Order Date/Time Bucket	Card Brand
0.49	$1,166,897	IP Region Risk	Product/Service Bucket	Item Count Risk Bucket	Email Domain Risk Group	IP Proxy
0.49	$1,133,723	IP Region Risk	Product/Service Bucket	Item Count Risk Bucket	IP Type	Order Date/Time Bucket
0.48	$1,115,112	IP Region Risk	Geo-Location Consistency	Product/Service Bucket	Email Domain Risk Group	Card Brand
0.49	$1,108,703	IP Region Risk	Geo-Location Consistency	Product/Service Bucket	IP Type	Card Brand
0.49	$1,107,996	IP Region Risk	Product/Service Bucket	Email Domain Risk Group	Geo-Location Distance	Card Brand
0.49	$1,094,666	IP Region Risk	Product/Service Bucket	Geo-Location Consistency	Email Domain Risk Group	Card Brand

B

Cost	Fraud Reduction	Dimension 1	Dimension 2	Dimension 3	Dimension 4	Dimension 5
0.49	$2,140,908	Usage Data Bucket	IP Region Risk	IP Type	Card Brand	Product/Service Bucket
0.49	$2,090,128	Usage Data Bucket	IP Region Risk	Geo-Location Consistency	IP Type	Product/Service Bucket
0.49	$2,082,986	Usage Data Bucket	IP Region Risk	Item Count Risk Bucket	Email Domain Risk Group	Product/Service Bucket
0.49	$2,064,067	Usage Data Bucket	IP Region Risk	Item Count Risk Bucket	IP Type	Product/Service Bucket
0.49	$2,045,565	Usage Data Bucket	IP Region Risk	IP Proxy	Card Brand	Product/Service Bucket
0.49	$2,034,346	Usage Data Bucket	IP Region Risk	Email Domain Risk Group	IP Type	Product/Service Bucket
0.49	$2,033,195	Usage Data Bucket	IP Region Risk	Geo-Location Consistency	IP Type	Product/Service Bucket
0.49	$2,025,677	Usage Data Bucket	IP Region Risk	Phone Velocity	Email Domain Risk Group	Product/Service Bucket
0.48	$2,022,095	Usage Data Bucket	IP Region Risk	Item Count Risk Bucket	Card Brand	Product/Service Bucket

Solution: Data Mastery

Key is to measure the right things and find the combinations that yield optimal results.

Usage Data Bucket	IP Region Risk	Phone Velocity	Email Domain RG	Product Bucket
15%	20%	7%	20%	17%

0.10%	0.13%	0.17%	0.53%	0.24%	0.40%	0.30%	0.28%
0.26%	0.77%	1.50%	1.00%	0.97%	3.24%	1.36%	1.16%
0.51%	0.47%	0.71%	0.96%	0.44%	1.11%	0.51%	0.64%
1.09%	5.69%	2.93%	0.97%	3.49%	7.01%	4.05%	2.75%
2.16%	2.89%	5.23%	3.29%	3.88%	21.53%	18.33%	13.66%
2.62%	3.78%	4.38%	3.37%	4.22%	4.71%	4.40%	3.71%
2.96%	5.34%	5.25%	2.67%	6.62%	17.46%	10.10%	9.04%
6.49%	5.92%	4.83%	4.65%	10.68%	14.14%	9.94%	6.67%
7.56%	10.70%	6.37%	3.79%	5.16%	32.63%	22.35%	21.42%
8.52%	5.87%	7.93%	5.66%	4.19%	21.07%	12.10%	8.97%
12.36%	22.71%	30.61%	20.86%	21.22%	0%	0%	0%
12.58%	8.86%	10.89%	6.03%	6.09%	6.30%	13.54%	0.96%

$600,000

70%

400 variables = trillions of combinations. Which lead to most powerful rules?

Cleaner Fraud: Implications

- Criminals are constantly developing new attack vectors.
- Criminals seek to maximize ROI on those investments by applying new attack vectors within an industry and then across industries.
- Criminals are always seeking merchants with weakest defenses. Don't be that merchant.
- Known "best practices" are becoming obsolete.
- An accelerating arms race.

Cleaner Fraud: Solutions

- Don't trust that existing systems and processes will work in the future, just because they worked in the past.
- Develop early warning indicators and monitor them daily to detect new attacks that might be circumventing current controls.
  - Chargeback volumes and characteristics.
  - New-account signup velocity, characteristics, clusters.
  - Authorization declines, especially fraud related.

Cleaner Fraud: Solutions

- Strategies that are harder for criminals to circumvent.
- Use deeper data to inform risk decisions.
  - Behavior before/after purchase transaction.
  - Account source data.
- Join customer-provided data with third party data.
  - IP, Machine, Phone, Name/Address, Social Network.
- Use analytics to refine fraud rules.
  - Complex rules that are harder to evade.
  - Fine tune manual review vs false positives vs fraud.

Contact

Mitch Muroff

CEO

Curaxian Inc.

mitch@curaxian.com

Denise Aptekar

Director, Trust & Safety

oDesk

daptekar@odesk.com