

# Machine Learning for Fraud

Brendan Herger, [hergertarian.com](http://hergertarian.com)

Slides: <https://goo.gl/cjW7jn>



MAN, I SUCK AT THIS GAME.  
CAN YOU GIVE ME  
A FEW POINTERS?

0x3A28213A  
0x6339392C,  
0x7363682E.

I HATE YOU.









Observations  
Feature engineering  
Models



# Observations

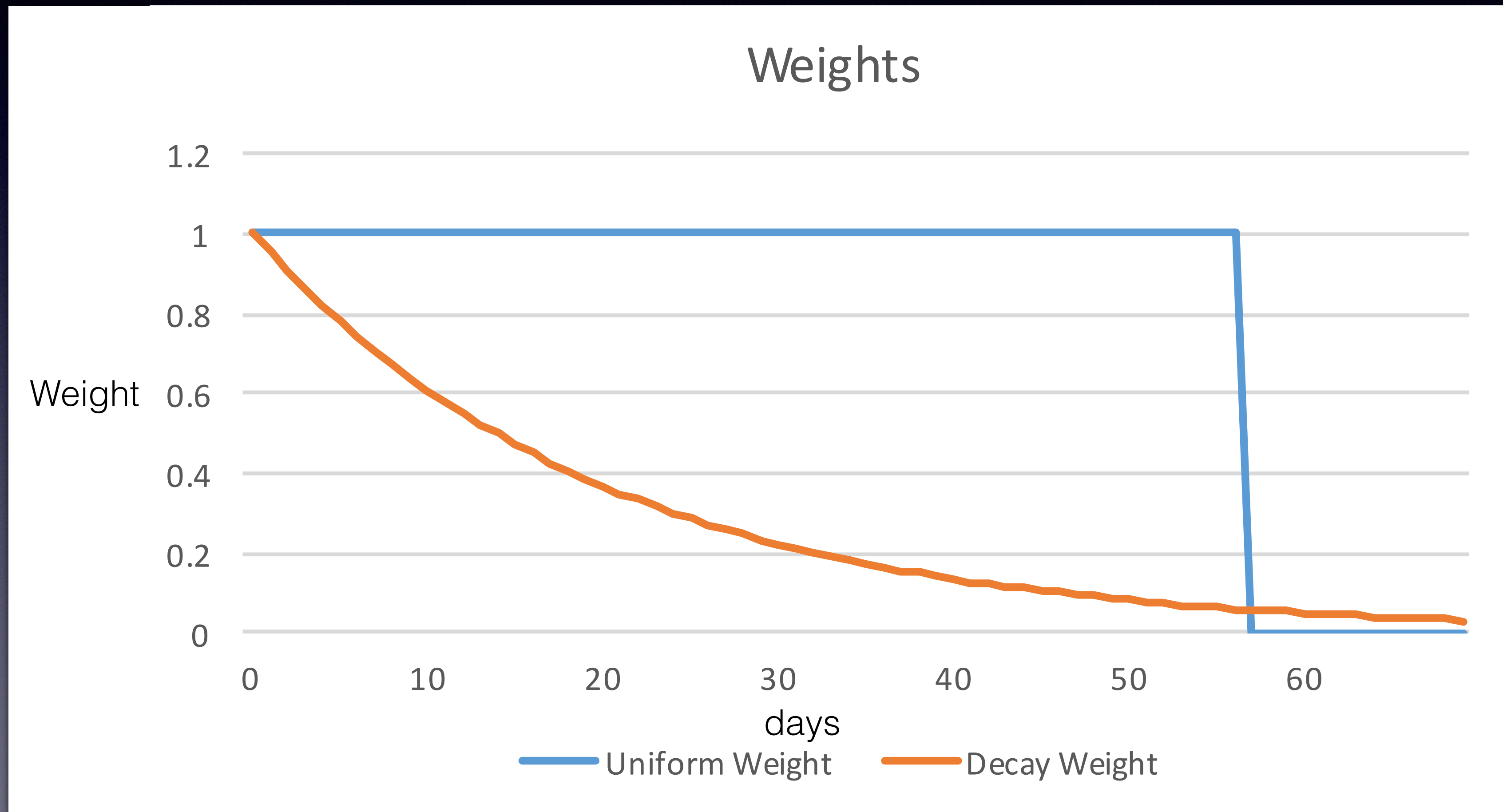


# Observation Weighting

- Re-weight observations, based on:
  - Uniform weight
  - Observation age (staleness)
  - Random down-sampling (randomly set weight to 0)
  - Up-sampling known opponent attacks (raise weight for known attacks)



# Observation Weighting





# SMOTE

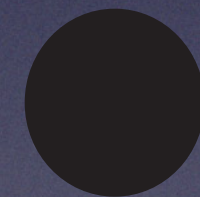
(Synthetic Minority Over-sampling Technique)

- Create synthetic observations, similar to actual attacks
- **Goal:** Better model rare events (opponent attacks)
- **Method:**
  - Majority class: Down sample, with some probability
  - Minority class: Create 'synthetic' observations



# SMOTE

1. Select minority point
2. Select neighbor
3. Create new point





# SMOTE

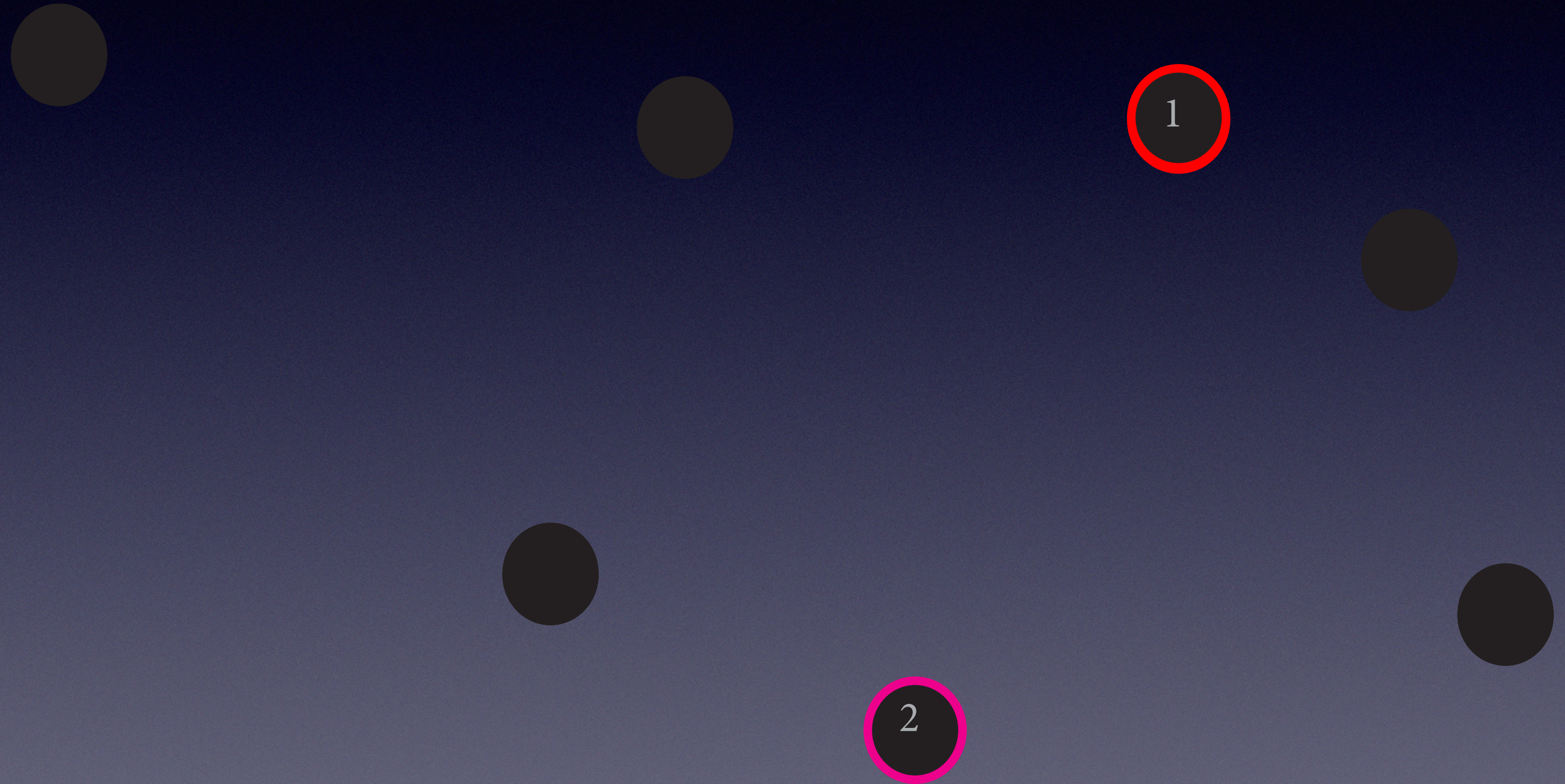
1. Select minority point
2. Select neighbor
3. Create new point





# SMOTE

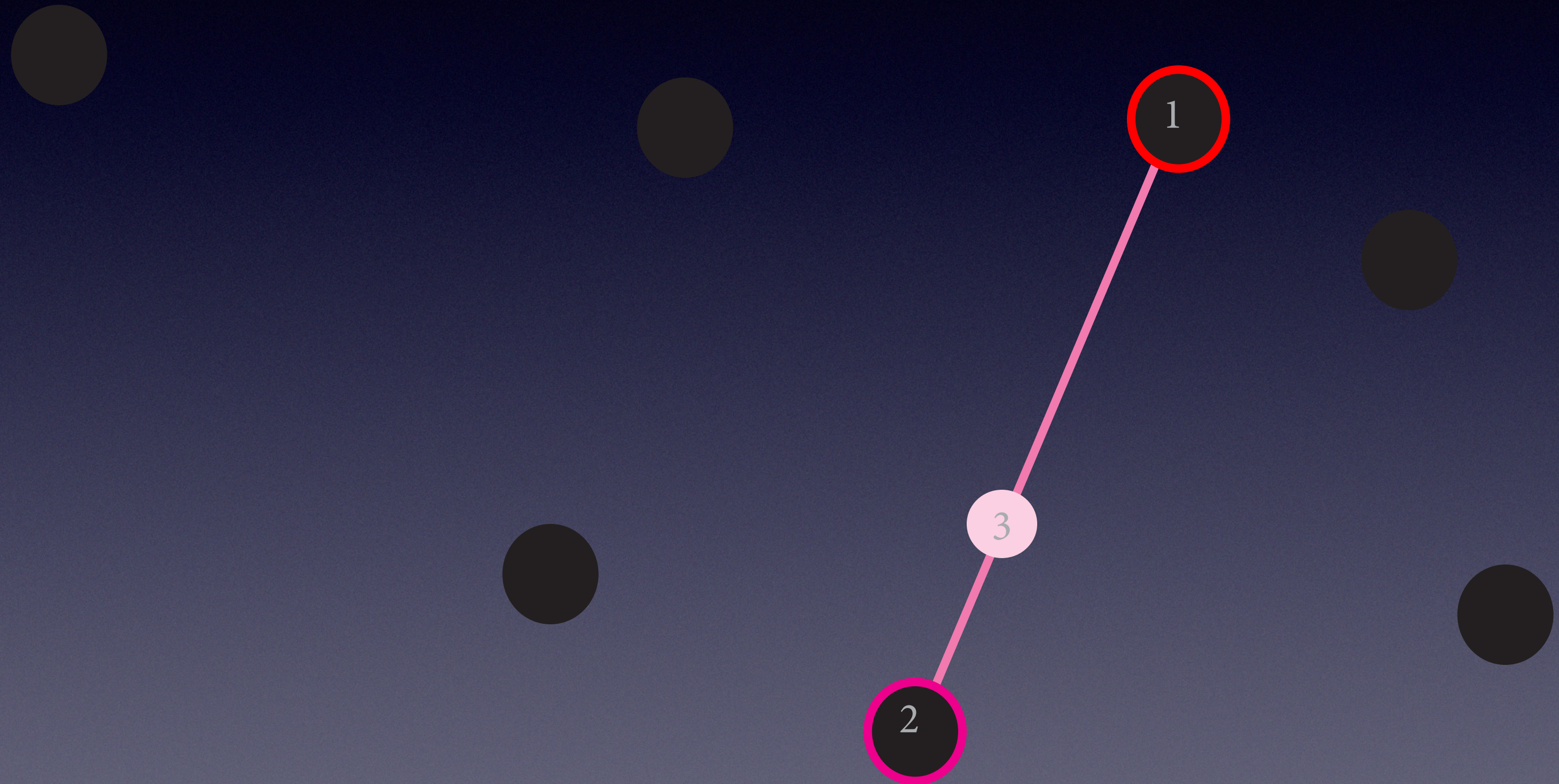
1. Select minority point
2. Select neighbor
3. Create new point





# SMOTE

1. Select minority point
2. Select neighbor
3. Create new point





# Observation Weighting SMOTE Sampling







# Feature engineering

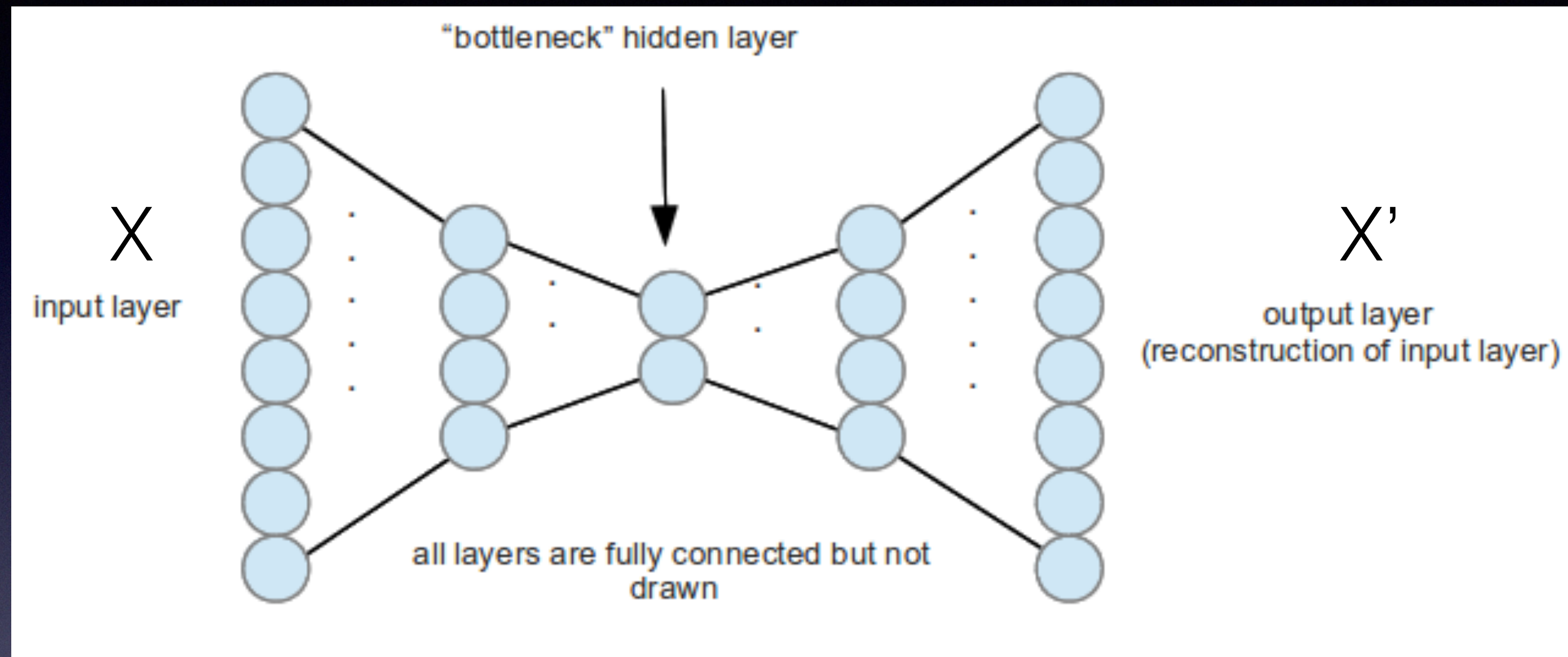


# Outlier Detection

- **Goal:** Create outlier score
- **Method:** Train learner to re-create input vector
  - PCA: Reduce dimensionality, increase dimensionality
  - Neural Network: Train auto-encoder, with bottleneck
- **Score:** Measure distance from output vector to input vector



# Outlier Detection



Outlier score:  $|X' - X|$



# Microclustering

- **Goal:** Capture what is 'normal' for this user
- **Method:**
  - Cluster users into small cohorts of similar users
  - Train a model for each cohort
- **Score:** Fraud likelihood score for user's cohort



# Historical aggregates

- **Goal:** Capture what is 'normal' for this user
- **Method:** Perform aggregates for various time windows
  - E.g. Average spend for past 30, 60, 90 days
  - E.g. Maximum spend for past 30, 60, 90 days

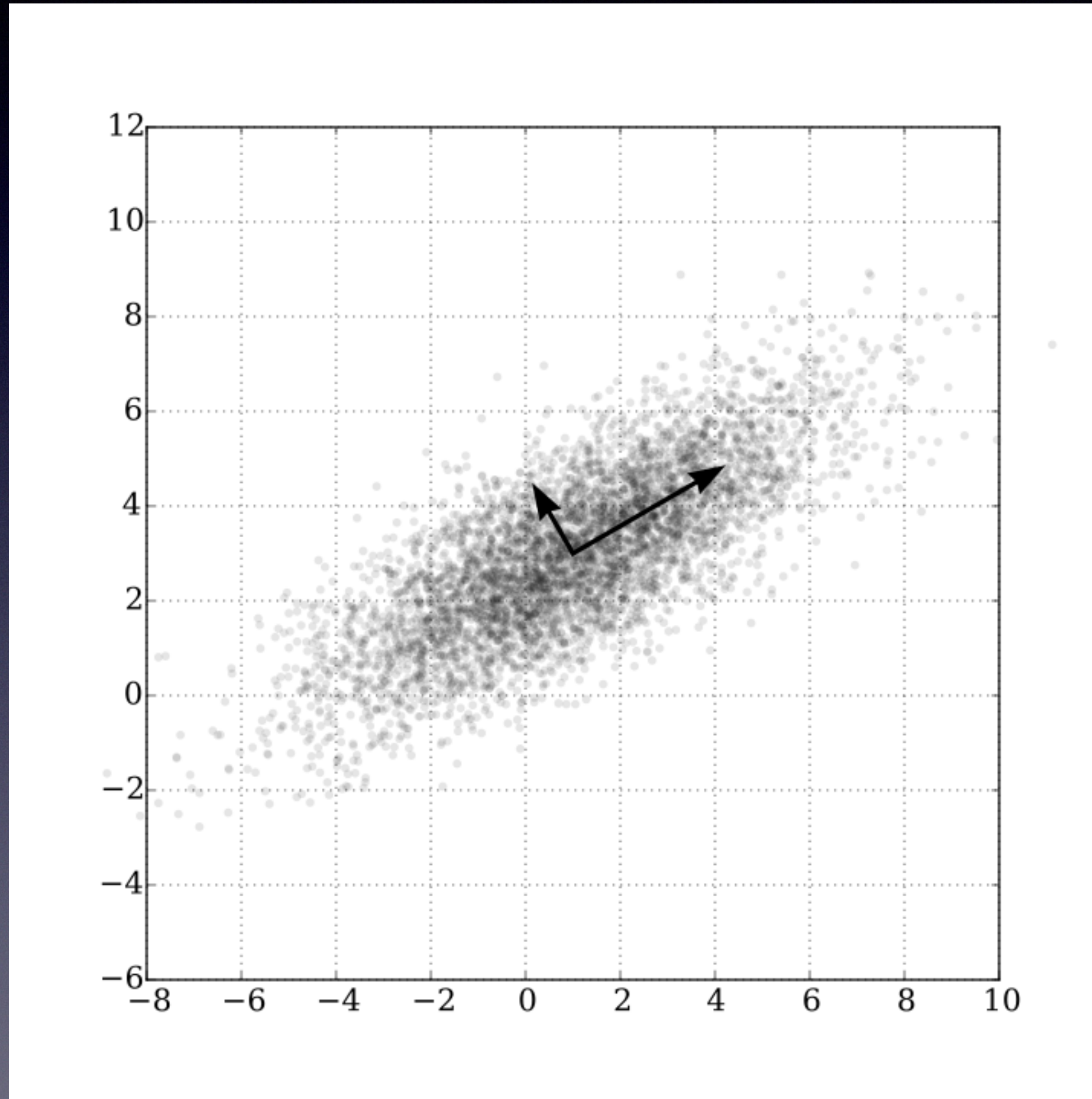


# Low Rank Models

- **Goal:** Reduce dimensionality, to include sparse or previously unused variables
- **Method:** Reduce dimensionality with generalized PCA
  - Model directly on components (latent factors)



# Low Rank Models



<https://web.stanford.edu/~boyd/papers/pdf/glrm.pdf>  
<https://github.com/h2oai/h2o-tutorials/blob/master/tutorials/glrm/glrm-tutorial.md>



Outlier Detection  
Microclustering  
Historical aggregates  
GLRM







# Models



# Grid search

- **Goal:** Find optimal hyper-parameters for given class of models
- **Method:** Create every possible permutation of hyper-parameters, and compute models until heat death of universe



# Neural Networks

- **Goal:** Deep, non-linear models perform well with rare cases
- **Method:** Try many different architectures, with many different hyper parameters
  - Feed previous user transactions to Bidirectional LSTM
  - Auto-encoder

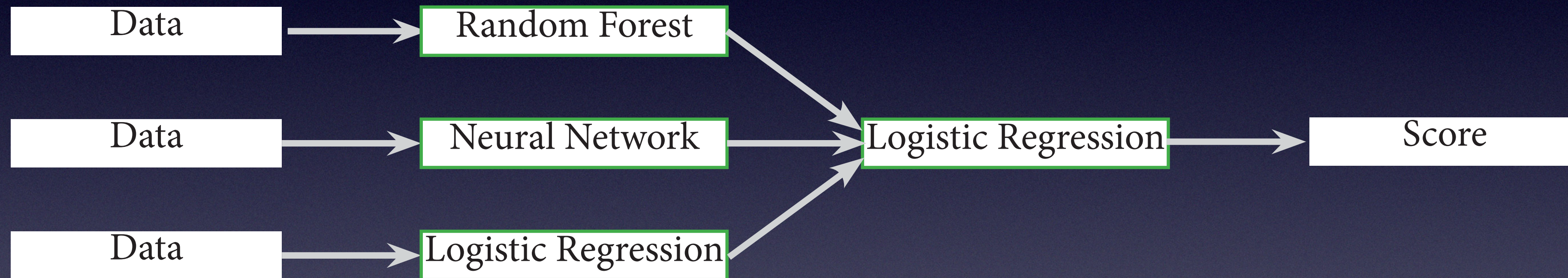


# Ensemble Modeling

- **Goal:** Leverage a diverse set of algorithms
- **Method:** Train multiple classes of algorithms (tree based, linear, neural network), possibly with multiple hyper-parameters. Combine scores with meta model (such as Logistic Regression w/ non-negative betas)



# Ensemble Modeling





Grid Search  
Neural Networks  
Ensemble models







# Thanks!

Brendan Herger, [hergertarian.com](http://hergertarian.com)

Slides: <https://goo.gl/cjW7jn>