Application Fraud
An attacker's introduction

Cory Scott
Matasano Security

cory@matasano.com / @cory_scott

Money for nothing

- Threat actor -> Vulnerability -> Loss
- Fraud is a loss outcome with:
  - Specific intent by the attacker
  - Financial gain achieved by the attacker
  - Direct loss incurred by the victim
- There are also attacks that are precursors to fraud (such as data breaches and malware infections); not in scope for today

And your checks for free

- Embezzlement
- Kickbacks
- Theft of product
- Theft of service
- Check and payment fraud
- Payment card fraud
- Payroll fraud
- Mortgage fraud
- Tax evasion
- Securities fraud
- Identity theft
- Insurance fraud
- Billing fraud
- Incentive and expense fraud
- Confidence schemes
- Transaction manipulation
- Counterfeiting
- Affiliate and marketing fraud
- Wire & mail fraud
- Telephone fraud
- Corporate Account Takeover
- Acquaintance fraud

- * NOT an exhaustive list

Look at them yo-yos

- ACH Fraud – Patco/Ocean Bank (2009)
  - $532k of fraudulent transfers on bank account and line of credit; $345k still missing after recovery efforts
- Sociètè Gènèrale trading fraud (2008)
  - $7.2bn loss due to a “rogue trader” entering non-existent hedges
- SWReg theft (2008-9)
  - $275k fraud: undisclosed flaw(s) in application allowed fake royalty credits to be entered and payment redirection to take place
- RBS Worldpay (2008)
  - $9m loss due to SQL injection attack against prepaid payroll debit card system

That's the way you do it

- Impersonation
  - Textbook example: Online banking systems.
  - Vectors: Malware, acquaintances, network intrusion, poor credential management, and application vulnerabilities.
- Abuse of trusted role
  - Textbook example: Front and back-office applications.
  - Vectors: Validation checks missing, insufficient monitoring, ability to modify or revert and obscure transactions, development/operations backdoors, and application vulnerabilities.

Them guys ain't dumb

- Lack of controls in application
  - Textbook example: Applications with a high frequency of transactions and a complex access control model.
  - Vectors: Insufficient requirements, mobile applications, and implementation vulnerabilities.
- Underlying compromise through or under application
  - Textbook example: Almost any application.
  - Vectors: Application vulnerabilities, malware, network intrusion, and abuse of privileged system/network access.