Synthetic Fraud

Susan Landauer, CPA

Forensic Accounting Services Group, LLC

Agenda

- What is synthetic fraud?
- The statistics of synthetic fraud
- How does synthetic fraud occur?
- How can credit unions defend against this fraud?

Synthetic Fraud

- Also called synthetic-identity fraud
- The criminal creates a fictional identity
- Fabricates a credit file by applying for a loan
- The identity gains credibility
  - However, there is no legitimate account holder

Statistics

- No true estimates can be found:
  - Synthetic fraud may account for 5% of uncollected debt and up to 20% of credit losses - $6 billion in 2017
  - Another study shows that synthetic fraud accounted for $5 billion in losses in 2014
- This is an 8 times increase from 2012
- Large number with store credit cards and auto loans
- Accounts for 20% of all credit cards losses
- Accounts for 1/5 of credit card charge-offs
  - Refunds over the past 3 years totaled $20 million

Fabricating the Credit File

- When an applicant applies for a source of credit – the CRAs (credit reporting agencies) (TransUnion, Experian and Equifax) scour the system looking for a match when a file is sent in
- In none found, a file is created by the CRAs to track this "inquiry"
- ***Key – if no records or matches are found – a file is created to track this!***
- Likely to be denied to begin with, but as more applications are made, the credit file grows
- Usually can obtain a credit-building card with a low limit ($300-$500)
  - Fraudsters pay these off to slowly build credit

Fabricating the Synthetic ID

- Obtain a SS# of another person
- Fabricate a name to be used with the SS#
- Create false births that are close to the fraudsters – to match if they ever have to appear
- Create an address to receive mail
- Provide stale or old telephone numbers
- Open accounts
- Make payments
- Exploit at the maximum time

On the Rise…

- Was generally committed by consumers with poor credit ratings
- Now is a wide spread criminal activity

- 2013 – the US Attorneys Office for New Jersey charged 18 defendants with plotting a $200 million credit card fraud conspiracy that involved fabricating more than 7,000 identities to obtain tens of thousands of credit cards

- WHY?!?!
  - Data breaches
  - Method of issuing SS#'s
  - New Credit Card technology

Schemes

- Apply for a loan with a lender
- Authorized Users
- Bust out schemes
- Data furnishing

Applying for a Loan

- Real Social Security numbers used:
  - A deceased person
  - An elderly person who is not seeking new credit
  - A child's stolen Social Security number
    - Children targeted because they are inactive and in general remain unchecked until they reach 18 – 51 times more likely to use a child's SS# (according to a Carnegie Mellon study)
  - Uses a made-up Social Security number

Authorized Users

- Also known as “piggybacking”
- Fraudsters actively recruit cardholders with good credit to add unknown people/identities to their existing credit
  - They believe they are helping others to establish or repair their credit
- A legitimate card holder adds an additional user, for a fee, to his/her account
- Credit card doesn’t even have to be issued or used
  - Aids in the establishment of the credit file
  - The additional user inherits the original card owner’s credit history
- Fraudster then applies for multiple lines
  - Maxes them out buying electronics and gift cards
- There are brokers to match people willing to share with fraudsters
  - Some have added as many as 50 to their account

Bust-Out Schemes

- Credit lines are maxed out
- Then paid down with worthless or counterfeit checks
- Maxed out again before checks do not clear

Example

- Synthetic ID was created in June 2014
- Used an address tied to a retail shopping center
- A trade line with a credit limit of $55,000 was added to the synthetic ID
- Within 2 months of adding the authorized user, synthetic id had $200K in unsecured credit
- Most purchases made were retail gift cards and high end merchandise

Data Furnishing

- Requires more sophistication and organization
- May involve complicit insiders within a small business
- Fraudsters us a front company that is approved to furnish or supply payment history on credit accounts
- Could be new companies or existing companies that have been compromised by an organized fraud ring
  - “Applicant” is granted credit for a fictitious purchase from the business
  - The business reports payments on the credit account associated with the synthetic identities to which it provided “credit”
  - The credit score improves…allowing the fraudsters

Red Flags

- Stolen children's Social Security number
  - Calls from bill collectors
  - Credit card offers arrive in the mail for the child
  - Child is denied a driver's license or college loan
  - Difficulty in getting first job – bad credit check

Red Flags –Data Furnishers

- CRAs tie multiple synthetic ids to the businesses
- Credit granted exceeds the normal price of goods from the vendor’s line of business

Prevention of Synthetic Fraud

- Some financial institutions are requiring customers / members to actually show up at a branch for any loans applied for
- Artificial intelligence
  - Using social media to confirm existence of member
    - Facebook, yearbooks, community data
- Industry – wide solution?
  - EWS – Early Warning Services – implemented 25 years ago to combat identity theft
- Voice recognition software at call centers
  - Determine if the voice has called in before for a different account

Questions??

Slandauer@forensicasg.com