Financial Services Industry: Identity Validation Use Cases

March 7, 2016
Capital One
US Card Fraud
Authentication is critical to prevent criminal activity during remote interactions between financial institutions and individuals.

<table>
<thead>
<tr>
<th>Remote Interaction Channels</th>
<th>Traditional Authentication</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Phone</td>
<td>• Largely knowledge-based (e.g., non-public personal information, credit history)</td>
<td>• Personal information compromise</td>
</tr>
<tr>
<td>• Web</td>
<td>• Some uses of technology (e.g., phone number or IP matching)</td>
<td>• Proliferation of synthetic identities</td>
</tr>
<tr>
<td>• Mobile</td>
<td></td>
<td>• Masking or alteration of phone number or IP address</td>
</tr>
</tbody>
</table>
The prevalence of illicitly-obtained consumer personal data has made it easier for criminals to impersonate consumers.

Data breach at large US company (publicly disclosed Feb 2015)

- 80 million customers impacted
- Name
- Address
- Date of Birth
- Social Security Number
- Email Address

This one breach alone has impacted a number of people equivalent to one-quarter of the US population.

It is but one of many large-scale data breaches over the last 2-3 years.
The lack of accessible & reliable data repositories is an obstacle to validating that a set of identity elements represent a real person.

**Credit Bureaus**
- Captures consumer information regarding their identity and credit history
- Bureaus collect the data but do not necessarily verify its accuracy
- Simply applying for a loan can create a bureau record if one does not already exist for that identity

**SSA & IRS**
- “Official” sources which record the person to whom an SSN was assigned
- Narrowly-defined permissible uses of this data prevents its use for identity verification

**Other Data Vendors**
- Wide variety of data available beyond credit & identity, e.g.: phone number ownership, email ownership
- Coverage and accuracy of data varies, dependent on individual vendor practices
- Useful to supplement other large-scale data sources, rather than serving as a core data source
We will review two common use cases where financial institutions are challenged to authenticate an individual:

- Account Opening
- Account Servicing
Online Account Opening Process

**Complete Application Form**
- Applicant submits data into a web form to establish their identity and creditworthiness

**Evaluate Risk Indicators**
- Financial institution reviews applicant identity and evaluates credit and fraud risks

**Prompt for Additional Action**
- Financial institution may prompt the applicant for additional action, such as: providing proof of income, answering knowledge-based questions to verify identity, or providing documents to prove identity

**Render Final Decision**
- Based on all the information received, the financial institution renders a final approval or decline decision
Financial institutions are faced with three challenges relating to the identity of the applicant, before they can make a grounded decision

• **Is the applicant a real person?**
  – Simply finding a credit bureau record for the applicant does not prove he/she is a real person

• **Is the applicant the person submitting the application?**
  – Anyone with access to key pieces of consumer non-public personal information (NPI) can use that data to submit an application exactly as if they were that consumer
  – Some criminals will go so far as to obtain a credit report for their victim, so as to answer any knowledge-based questions that may be asked during the application process

• **Does the applicant’s credit history accurately reflect their creditworthiness?**
  – Account credit history is reported to the bureau for the account owner and its authorized users (AUs)
  – Effectively AUs “inherit” the account credit history even though they are not actually responsible for paying back that loan
Account Servicing Use Case – Adding an Authorized User (AU)

- Customer calls credit card issuer, with the intent of adding their college-age child as an Authorized User (AU)

- Customer provides information (e.g., SSN, DOB, card security code on back of card) to pass authentication requirements to access their account

- An AU is added to the account, along with some identifying information (name, DOB, etc.) in case that AU calls in for servicing in the future

- Customer requests that the AU plastic be sent directly to their child's college address, which is away from home
Issuers face several challenges in validating the identity of a caller purporting to be a customer

- **Knowledge-based authentication is becoming less effective as criminals gain access to more victim data**
  - Non-public personal information (SSN, DOB, mother’s maiden name)
  - Credit bureau data (loans opened, previous addresses, public records)

- **Criminals are finding ways to circumvent authentication via outbound communication**
  - **Phone Calls**: Criminals can use the victim’s NPI to take over the victim’s telco account and forward calls to their own number
  - **Text Messages**: Criminals can take over the victim’s wireless account to receive blind carbon copies of all texts sent to the victim
  - **Email**: Criminals can phish or otherwise compromise the victim’s email to intercept communications to the victim

- **Biometric authentication could be promising but has practical limitations**
  - Voice recognition technology can be hindered by poor phone connections, reasonable variations in voice (e.g., cough/cold), or background noise
The path to overcome the challenges around identity validation requires a multi-pronged approach

**Consumer Awareness**
- Educate about elevated exposure to identity theft
- Encourage increased vigilance of personal data (e.g., review your free credit reports regularly)
- Motivate adoption of new authentication technologies as they are made available

**Data Repositories**
- Credit bureaus should do more to validate the accuracy of data collected
- Trusted entities (e.g., government agencies, federal agencies, etc.) create centralized identity validation services for use by certified entities

**Authentication Technology**
- Foster development of new technology which is simple for consumers to use and difficult for criminals to circumvent
- Support the implementation of new technologies in the most vulnerable & critical economic sectors