UA Identity Theft Prevention Program—Records & Information Security Management

Dr. Russell O’Hare
Chief Records Officer

Presented to: Board of Regents Audit Committee

February 20-21, 2014
Contents Covered

- University of Alaska - Records and Information Management
- Information Governance
- Identity Theft
- Protecting Personally Identifiable Information (PII) at UA
- Federal Trade Commission Fair and Accurate Credit Transaction (FTC FACTA) Red Flags
- Board of Regents – Approved ID Theft Prevention Program
- Red Flag – UA Identity Theft Prevention Program
- Adak Island: Unauthorized access to student & employee PII
- Enterprise Content Management – OnBase
- References

www.alaska.edu/records
Records & Information Management Mission

- Ensure compliance
- Information Governance
- Enterprise Content Management
What is Identity Theft?

The theft or misuse of personal identifying information in order to gain something of value or facilitate other criminal activity.

Alaska State Statute § 45.48 – Personal Information Protection Act

to obtain, possess, transfer, or use a person’s “identifying information” with the intent to harm the person.
Identity Theft Complaints

Source: Federal Trade Commission, February 2013 - Consumer Sentinel Network

Complaint Types
- Identity Theft Complaints
- Other Complaints
- Fraud Complaints

www.alaska.edu/records
Maximum ID Theft Victims: Age 20-29

Source: Federal Trade Commission, February 2013 - Consumer Sentinel Network

- Maximum number of victims belong to Age 20-29 years
- 70% of the victims are students or in early stages of careers
- Universities / Colleges have higher responsibility and need to be cognizant
- Records retention schedule and information governance in compliance with the regulations

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 and Under</td>
<td>6%</td>
</tr>
<tr>
<td>20 - 29</td>
<td>21%</td>
</tr>
<tr>
<td>30 - 39</td>
<td>19%</td>
</tr>
<tr>
<td>40 - 49</td>
<td>18%</td>
</tr>
<tr>
<td>50 - 59</td>
<td>17%</td>
</tr>
<tr>
<td>60 - 69</td>
<td>11%</td>
</tr>
<tr>
<td>70 and Over</td>
<td>8%</td>
</tr>
</tbody>
</table>
Most of the identity theft complaints in Alaska are reported in Anchorage and Fairbanks.
## ID Theft Contact and Payment (2012)

Source: Federal Trade Commission, February 2013 - Consumer Sentinel Network

### Fraud Contact Method

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail</td>
<td>38%</td>
</tr>
<tr>
<td>Mail</td>
<td>9%</td>
</tr>
<tr>
<td>Internet - Web Site/Others</td>
<td>12%</td>
</tr>
<tr>
<td>Phone</td>
<td>34%</td>
</tr>
<tr>
<td>Other</td>
<td>7%</td>
</tr>
</tbody>
</table>

### Fraud Victim Payment Method

<table>
<thead>
<tr>
<th>Payment Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank Account</td>
<td>14%</td>
</tr>
<tr>
<td>Cash/Cash Advance</td>
<td>7%</td>
</tr>
<tr>
<td>Check</td>
<td>8%</td>
</tr>
<tr>
<td>Credit Cards</td>
<td>17%</td>
</tr>
<tr>
<td>Money Order</td>
<td>6%</td>
</tr>
<tr>
<td>Telephone Bill</td>
<td>1%</td>
</tr>
<tr>
<td>Wire Transfer</td>
<td>47%</td>
</tr>
</tbody>
</table>
How is information stolen?

- Scams/fraud
- Trash diving
- Lost/stolen wallet/purse
- Mail theft
- Burglary
- Skimming
- Computer hacking
- Data breach
Identity Theft Information

- More than 10 million Americans are victims of identity theft each year.
- The total financial losses due to identity theft are estimated to be about $200 billion every year.
- The FTC received 369,132 complaints of ID theft in 2012, 18% of total complaints.
- When ID thieves opened new accounts victims spent an average of $1,865.
- Victims spent an average of $535-$2,350 in 2012 for damage to existing accounts.
RED FLAG RULES

Fighting Fraud at the University of Alaska by Protecting Student Personally Identifiable Information (PII)
Protecting Student Information requires
Compliance with:

- FERPA
- RED FLAG Rules - UA Identity Theft Prevention Program: approved by Board of Regents in 2009
- PCI
- Gramm-Leach-Bliley Act
- HIPAA
- Privacy Act of 1974
- Alaska Personal Information Protection Act AS 45.48
- Records Management: Security Breach Involving Personal Information R.05.08.023
Congress enacted the FTC FACTA of 2003 to help combat identity theft.

The final rules and guidelines became effective in 2009.

Section 114 of FACTA contains the Red Flag Rules that required UA to develop & implement a written Identity Theft Prevention Program.

The Rule supplements existing legislation aimed at preventing identity theft.

Applies to institutions and creditors with covered accounts.

Picks on where data security leaves off.
Overview of the Red Flags Rule

- What Are Red Flags?
  - Definition
    activity that could indicate a risk of identity theft
  - Purpose
    to detect and stop identity thieves
- Responsibilities
  protect against unauthorized access of personal identifiable information
UA Identity Theft Prevention Program

- Program approved June 5, 2009 by the Board of Regents
- Consistent with the Board of Regents Policy P.05.02.90 on financial fraud, waste and abuse
- Developed pursuant to the Federal Trade Commission’s (FTC) “Red Flags” Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act.
- Adds to compliance regulations from Dept. of Education
- Distinct from data security requirements
- Alaska State- Statute 45-48: Personal Information Protection Act

www.alaska.edu/records
UA Identity Theft Prevention Program

- Identify Red Flags
- Detect Red Flags
- Prevention & Mitigate Identity Theft
- Respond

www.alaska.edu/records
Red Flags & Current Security Protocol

- UA maintains protocols and procedures to address privacy of student and employee records & information, applying state and federal privacy laws.
- Data security also plays an essential role in keeping people’s information protected.
- Red Flag Rule picks up where data security leaves off, by working to prevent identity theft by ensuring institution has appropriate practices and protocol to identify risks, procedures to address those risks and prevent future risks.

www.alaska.edu/records
Identity Theft Prevention Workflow

**ID Committee / Administrators.**
- Notified possible Red Flag / Identity Theft.
- Monitor / Watch enrollment, existing accounts, Consumer Report Requests.

**Departments**
- Notified possible Red Flag / Identity Theft.
- Continue to Monitor.
- Move to mitigate potential damage.

**Customer**
- Authentic?
- Response Warranted?

**Campus Administrator**
- Process Incident Activities Report (IAR).
- Place hold on Credit Reports.

**Police / CR. Report Agencies**
- Notify Statewide Risk and General Counsel.
- Process IAR, Place hold on Credit Reports.

**SW PGM Admin**
- Notify Statewide Risk and General Counsel.

**Respond**
- Yes
- Cancel any transactions.
- Notified and informed how to respond.

**Prevent & Mitigate**
- Notified of Authentic Red Flag.

**Detect**
- Yes
- Process IAR.
## Sample – UA Incident Activity Report

<table>
<thead>
<tr>
<th>Red Flag Event / Suspicious Activity:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Campus(es) involved:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems compromised (if any):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date of Event(s):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee reporting the event</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Campus / Program Administrator recording IAR:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
</tr>
<tr>
<td>-------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of individual(s) potentially affected:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Has the suspicious activity had a material impact on, or otherwise affected the financial soundness of University of Alaska or one of its campuses?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Has Law Enforcement been contacted?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency name:</td>
</tr>
<tr>
<td>---------------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of person(s) contacted at Law Enforcement Agency(ies):</th>
</tr>
</thead>
</table>

### Individuals affected

<table>
<thead>
<tr>
<th>Name (Last, First)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID (30,xxx,xxx):</th>
</tr>
</thead>
</table>

| Email: | Phone: | Cell: |
Identity Theft Prevention & Red Flag Rule Implementation at UA

- Identity Theft Prevention Committee annually reviews the program.
  - Will reflect on lessons learned.
  - Will maintain an awareness of changes in identity theft methods, detection and prevention methods.
  - Oversee training

www.alaska.edu/records
Identity Theft Prevention - Training

- All University personnel shall be aware of the Identity Theft Prevention Program.
- Individuals working with Covered Accounts receive annual training.
- Individuals identified by a University Identity Theft Program Committee member shall undergo training on an annual basis.
- Training available via UAOnline/SkillSoft
In 2013, no instances of suspicious activities of covered accounts or incidents of identity theft.

The campuses’ report the program procedures have strengthened the protection of the university’s customer information.

There are no recommendations for modifying the program at this time.
University of Alaska – Identity Theft Prevention Program Guidelines

More details can be found in

https://www.alaska.edu/records/id-theft/

University of Alaska

Identity Theft Prevention Program

Effective beginning October 31, 2009
Adak Island: Records Security Incident

- Boxes of unsecured personal information from 1972-1994 discovered at abandoned former community college extension site (due to Base Realignment & Closure)
- UAA maintained the extension on military base in Adak & Shemya islands, enrolled approximately 5000 students during its operation
- Records badly deteriorated by water, unheated storage, aging in an abandoned building
- UA adopted new procedures for disposing of records when a campus, department, unit is decommissioned, reorganized or terminated
We did not steal any of these identities...
07-17-09
Montesano Washington
2-28-2010
UA implemented ECM system – OnBase almost a decade ago by adopting the state-of-the-art technology for the content management (capture, process, access, measure, integrate and store).

UA ECM Governance and Implementation Team – sets the guidelines on ECM deployment, process integration, access, data usage (restricted, internal, public), data retention.

Dr. Shiva Hullavarad
OnBase System Administrator,
Certified ECM& ERM Practitioner
OnBase Integration – Process Efficiency across University of Alaska

60% - Reduction in time to process Admission applications
80% - Reduction in Physical Space/Filing cabinet
80% - Reduction in time to process Graduation applications
References

- University of Alaska Identity Theft Prevention Program website: [http://www.alaska.edu/records/id-theft/](http://www.alaska.edu/records/id-theft/)
- FTC Red Flags website: [http://www.ftc.gov/redflagsrule](http://www.ftc.gov/redflagsrule)