The Chicago Approach To Identity Assurance

November, 2013 -- Identity Week CAMP

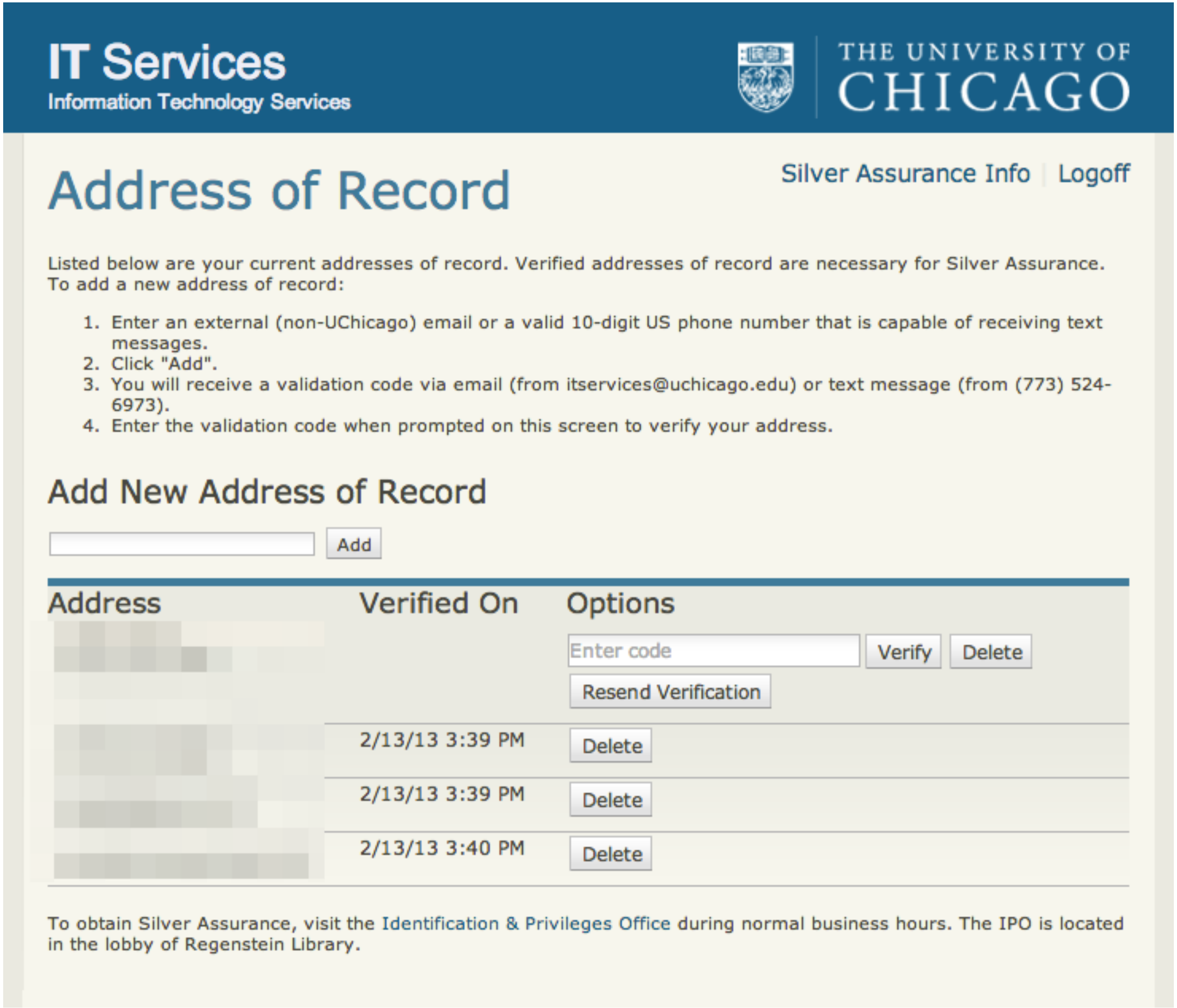
THE UNIVERSITY OF CHICAGO

Password Based

- Starting with just Faculty / Staff
- Passwords must be rotated on an annual basis
- Password >= 12 characters & follow complexity rules OR passphrase can be > 19 characters and not follow rules
- 90/5/5 Effective Bad Attempt Lockout Policy
  - Implemented as 9/5/5 lockout per node over 10 nodes

Attaining Silver Assurance

- Be Faculty or Staff
- Register Address of Record
- Bring Password into Compliance
- Present ID in person @ Identity Office



IT Services
Information Technology Services

THE UNIVERSITY OF CHICAGO

Address of Record

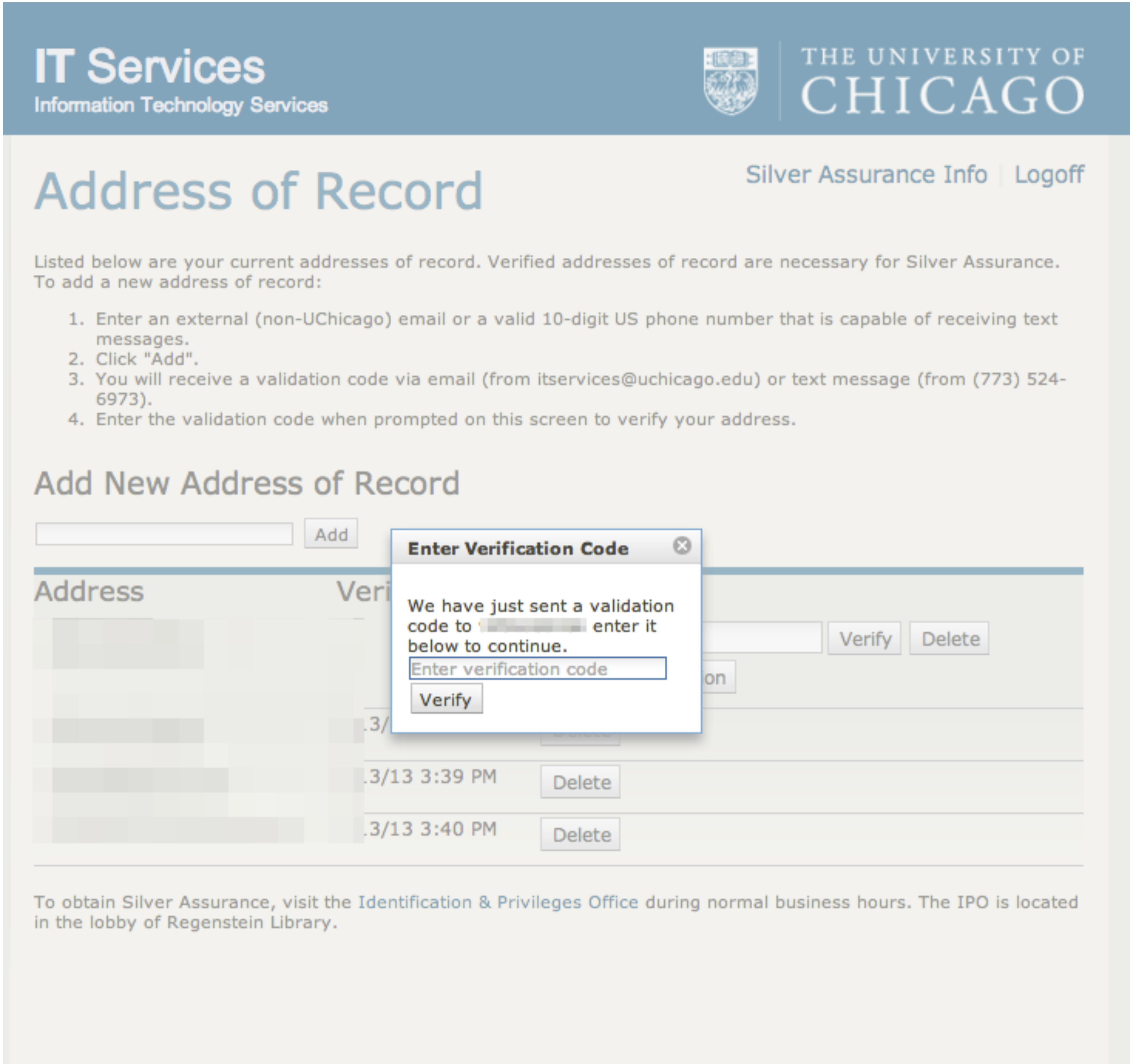
Listed below are your current addresses of record. Verified addresses of record are necessary for Silver Assurance. To add a new address of record:

1. Enter an external (non-UChicago) email or a valid 10-digit US phone number that is capable of receiving text messages.
2. Click "Add".
3. You will receive a validation code via email (from itservices@uchicago.edu) or text message (from (773) 524-6973).
4. Enter the validation code when prompted on this screen to verify your address.

Add New Address of Record

Address	Verified On	Options
[redacted]		Enter code Verify Delete Resend Verification
[redacted]	2/13/13 3:39 PM	Delete
[redacted]	2/13/13 3:39 PM	Delete
[redacted]	2/13/13 3:40 PM	Delete

To obtain Silver Assurance, visit the Identification & Privileges Office during normal business hours. The IPO is located in the lobby of Regenstein Library.



Address of Record

Listed below are your current addresses of record. Verified addresses of record are necessary for Silver Assurance. To add a new address of record:

1. Enter an external (non-UChicago) email or a valid 10-digit US phone number that is capable of receiving text messages.
2. Click "Add".
3. You will receive a validation code via email (from itservices@uchicago.edu) or text message (from (773) 524-6973).
4. Enter the validation code when prompted on this screen to verify your address.

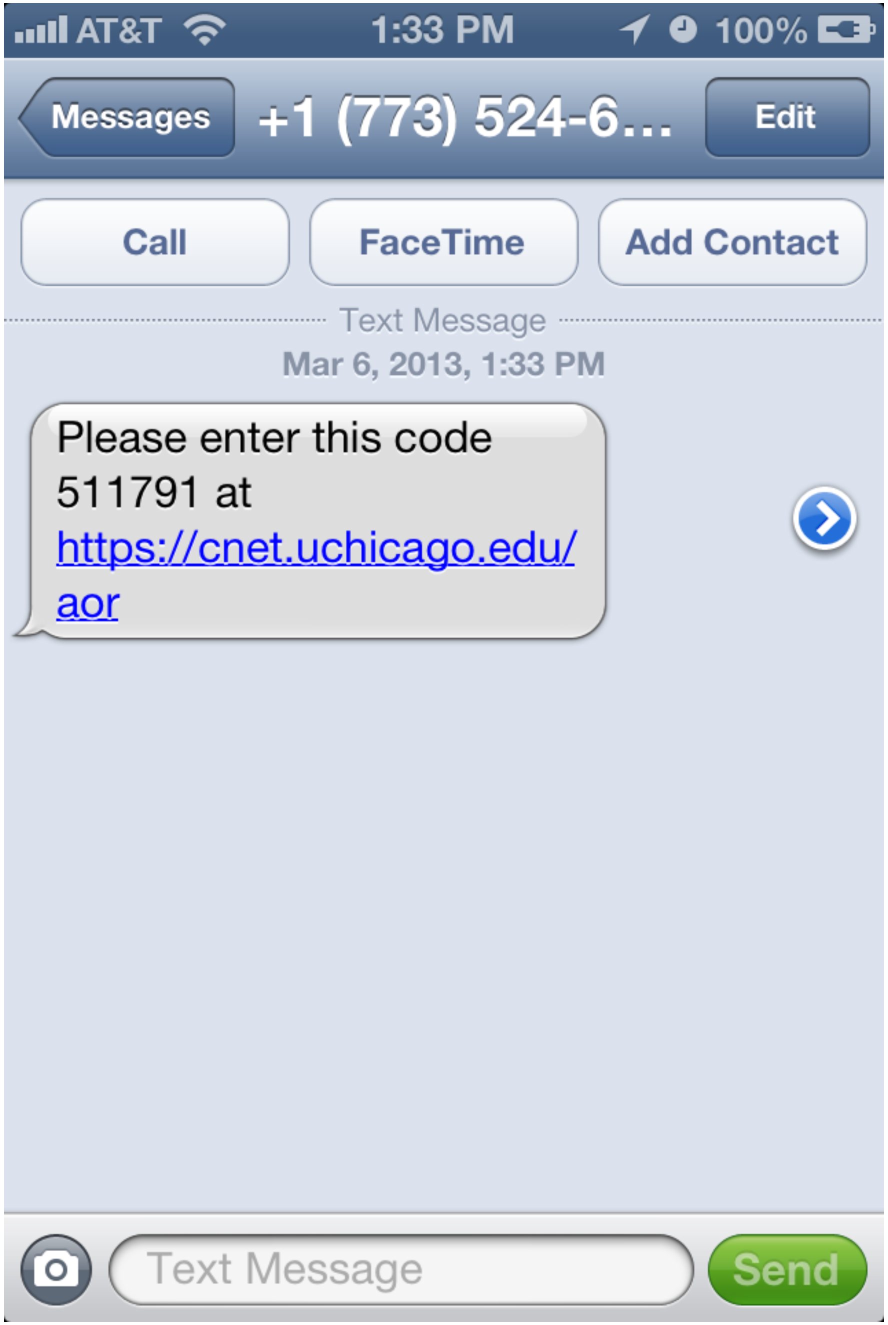
Add New Address of Record

Address	Veri	
[redacted]		Verify Delete on
[redacted]	.3/	
[redacted]	.3/13 3:39 PM	Delete
[redacted]	.3/13 3:40 PM	Delete

Enter Verification Code

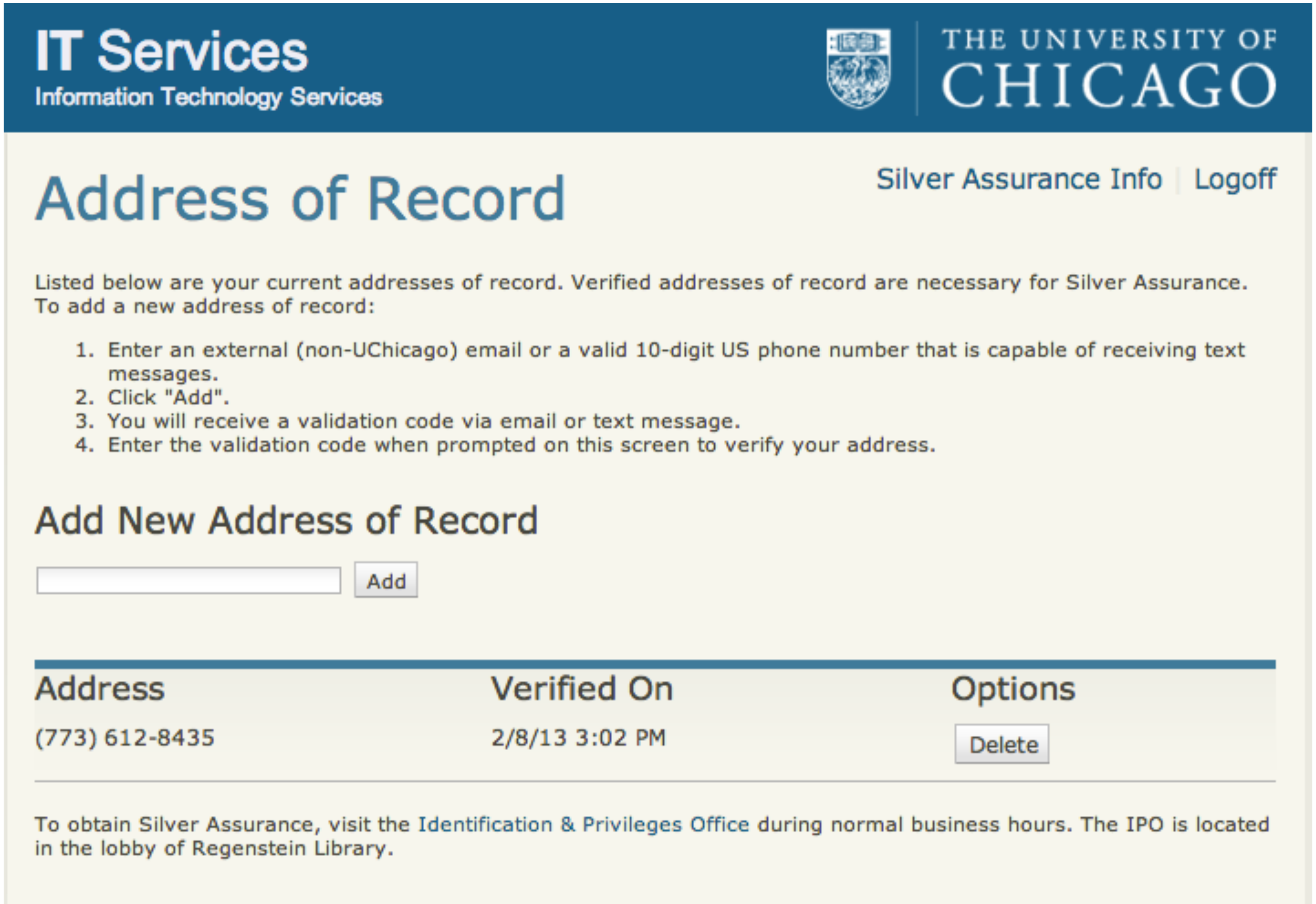
We have just sent a validation code to [redacted] enter it below to continue.

To obtain Silver Assurance, visit the Identification & Privileges Office during normal business hours. The IPO is located in the lobby of Regenstein Library.



Mar 6, 2013, 1:33 PM

Please enter this code 511791 at https://cnet.uchicago.edu/aor



IT Services
Information Technology Services

THE UNIVERSITY OF CHICAGO

Silver Assurance Info | Logoff

Address of Record

Listed below are your current addresses of record. Verified addresses of record are necessary for Silver Assurance. To add a new address of record:

1. Enter an external (non-UChicago) email or a valid 10-digit US phone number that is capable of receiving text messages.
2. Click "Add".
3. You will receive a validation code via email or text message.
4. Enter the validation code when prompted on this screen to verify your address.

Add New Address of Record

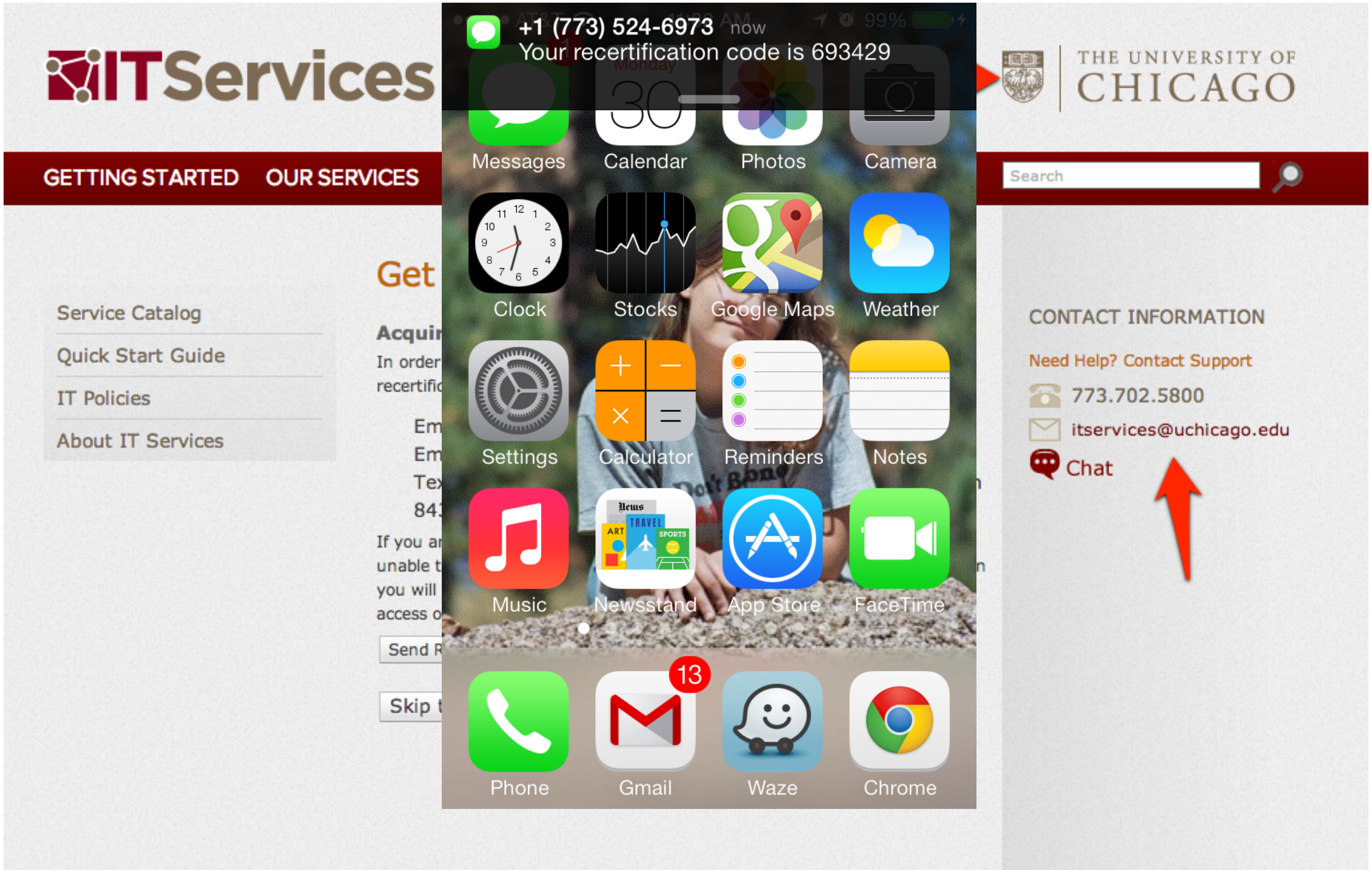
Address	Verified On	Options
(773) 612-8435	2/8/13 3:02 PM	Delete

To obtain Silver Assurance, visit the Identification & Privileges Office during normal business hours. The IPO is located in the lobby of Regenstein Library.

Password Rotation

- Annual
- To avoid any phishiness we send the user a calendar event set for 1 year from the date they set their password.
- Failure to rotate password results in loss of Silver until password is rotated. Access to non-silver resources is preserved.
- One-time code sent to external address is required to reset/rotate a password to Silver.

Password Rotation



+1 (773) 524-6973 now
Your recertification code is 693429

Get

Acqui

In order
recertific

Em
Em
Tex
84

If you a
unable t
you will
access o

CONTACT INFORMATION

Need Help? Contact Support

☎ 773.702.5800

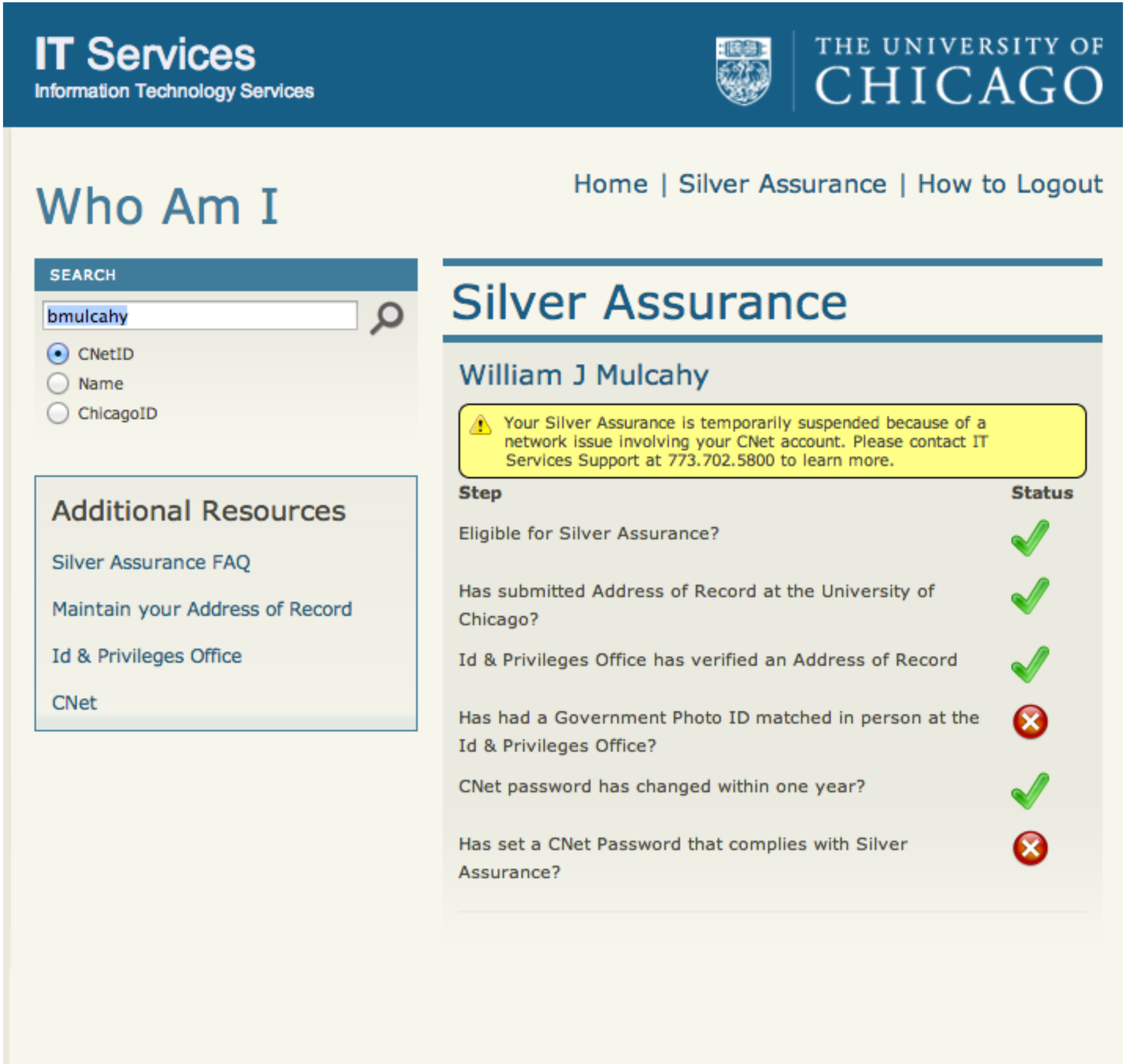
✉ itservices@uchicago.edu

Chat

THE UNIVERSITY OF CHICAGO

User Dashboard

- Allows user to view their Silver Assurance status
- Informs as to what steps still need to be taken to attain / restore Assurance


IT Services
Information Technology Services
THE UNIVERSITY OF CHICAGO
Home | Silver Assurance | How to Logout
SEARCH

Who Am I

SEARCH: bmulcahy

- ● CNetID
- ○ Name
- ○ ChicagoID

Additional Resources

- Silver Assurance FAQ
- Maintain your Address of Record
- Id & Privileges Office
- CNet

Silver Assurance

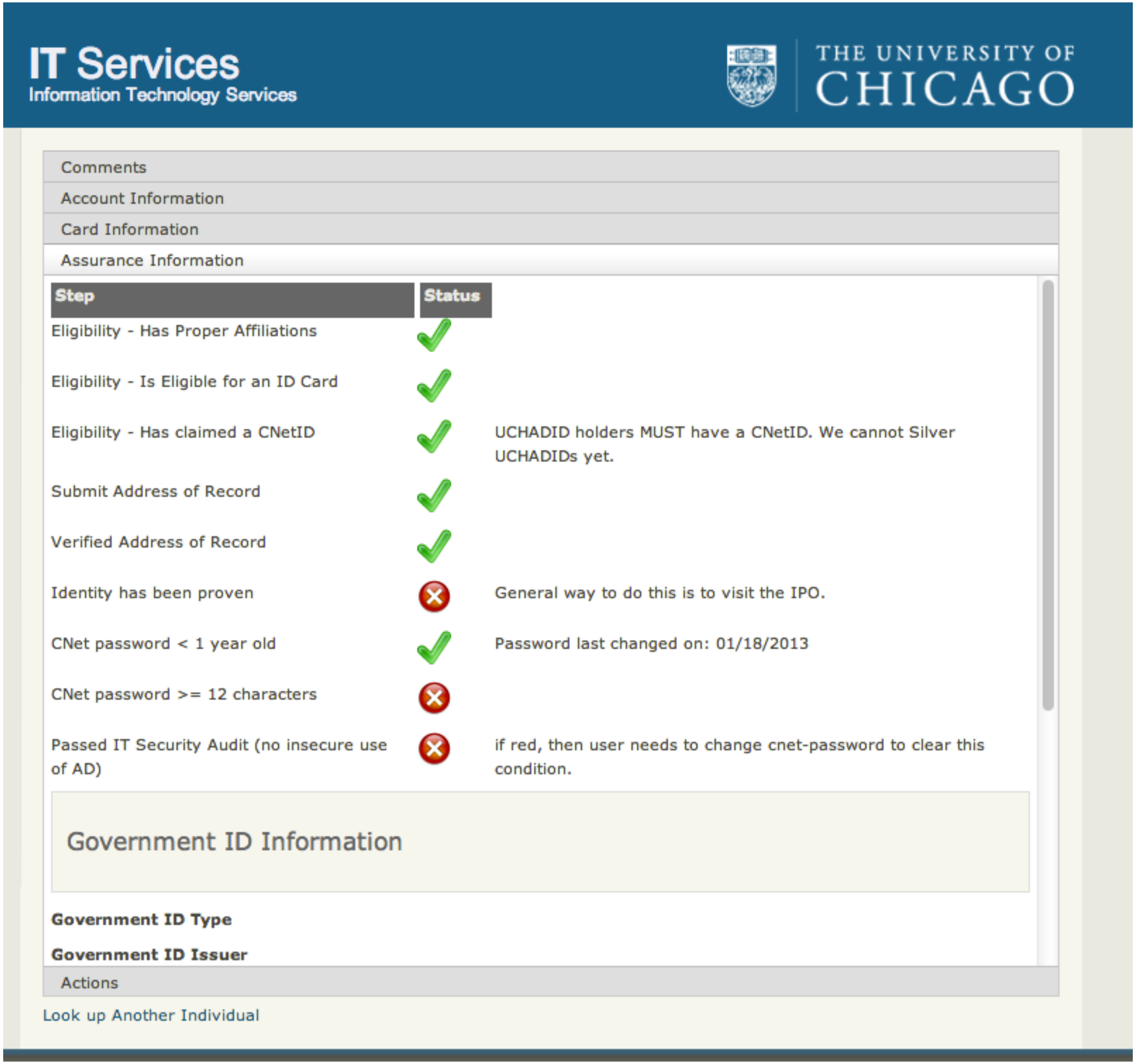
William J Mulcahy

⚠ Your Silver Assurance is temporarily suspended because of a network issue involving your CNet account. Please contact IT Services Support at 773.702.5800 to learn more.

Step	Status
Eligible for Silver Assurance?	✓
Has submitted Address of Record at the University of Chicago?	✓
Id & Privileges Office has verified an Address of Record	✓
Has had a Government Photo ID matched in person at the Id & Privileges Office?	✗
CNet password has changed within one year?	✓
Has set a CNet Password that complies with Silver Assurance?	✗

Admin Dashboard

- Used by support staff to diagnose Assurance issues
- provides more detail than user dashboard



Step	Status	
Eligibility - Has Proper Affiliations	✓	
Eligibility - Is Eligible for an ID Card	✓	
Eligibility - Has claimed a CNetID	✓	UCHADID holders MUST have a CNetID. We cannot Silver UCHADIDs yet.
Submit Address of Record	✓	
Verified Address of Record	✓	
Identity has been proven	✗	General way to do this is to visit the IPO.
CNet password < 1 year old	✓	Password last changed on: 01/18/2013
CNet password >= 12 characters	✗	
Passed IT Security Audit (no insecure use of AD)	✗	if red, then user needs to change cnet-password to clear this condition.

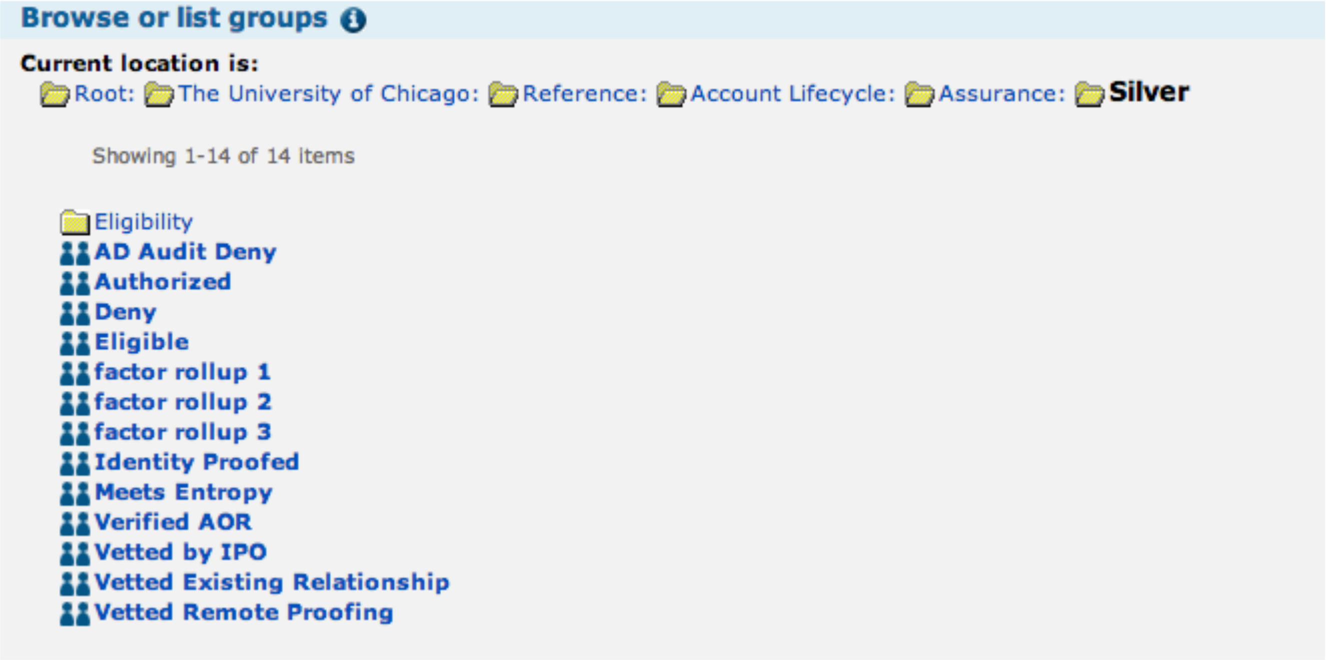
Government ID Information

Government ID Type

Government ID Issuer

Logic behind the calculation

- Grouper Based



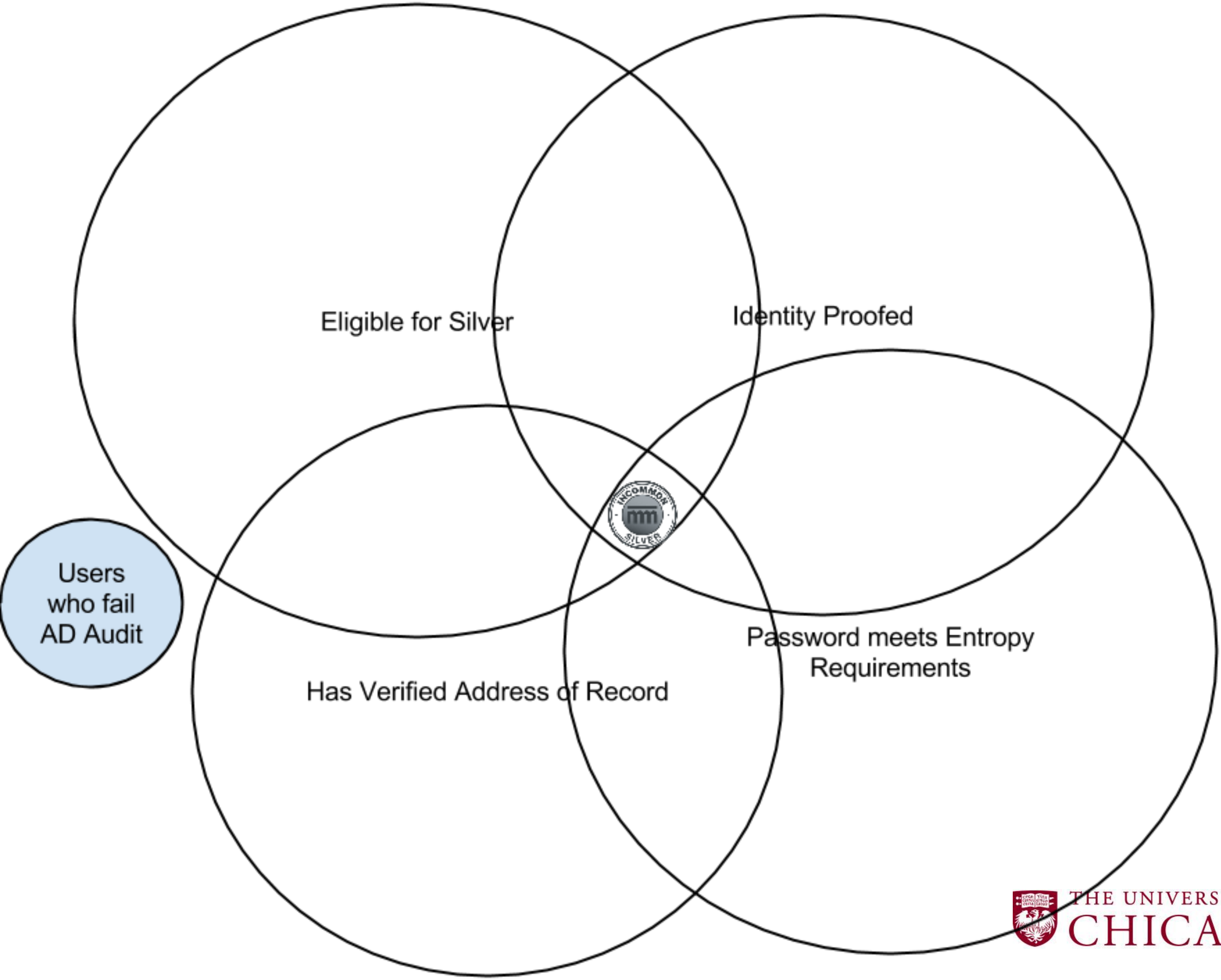
Browse or list groups

Current location is:

Root: The University of Chicago: Reference: Account Lifecycle: Assurance: **Silver**

Showing 1-14 of 14 items

- Eligibility
- AD Audit Deny
- Authorized
- Deny
- Eligible
- factor rollup 1
- factor rollup 2
- factor rollup 3
- Identity Proofed
- Meets Entropy
- Verified AOR
- Vetted by IPO
- Vetted Existing Relationship
- Vetted Remote Proofing



Eligible for Silver

Identity Proofed

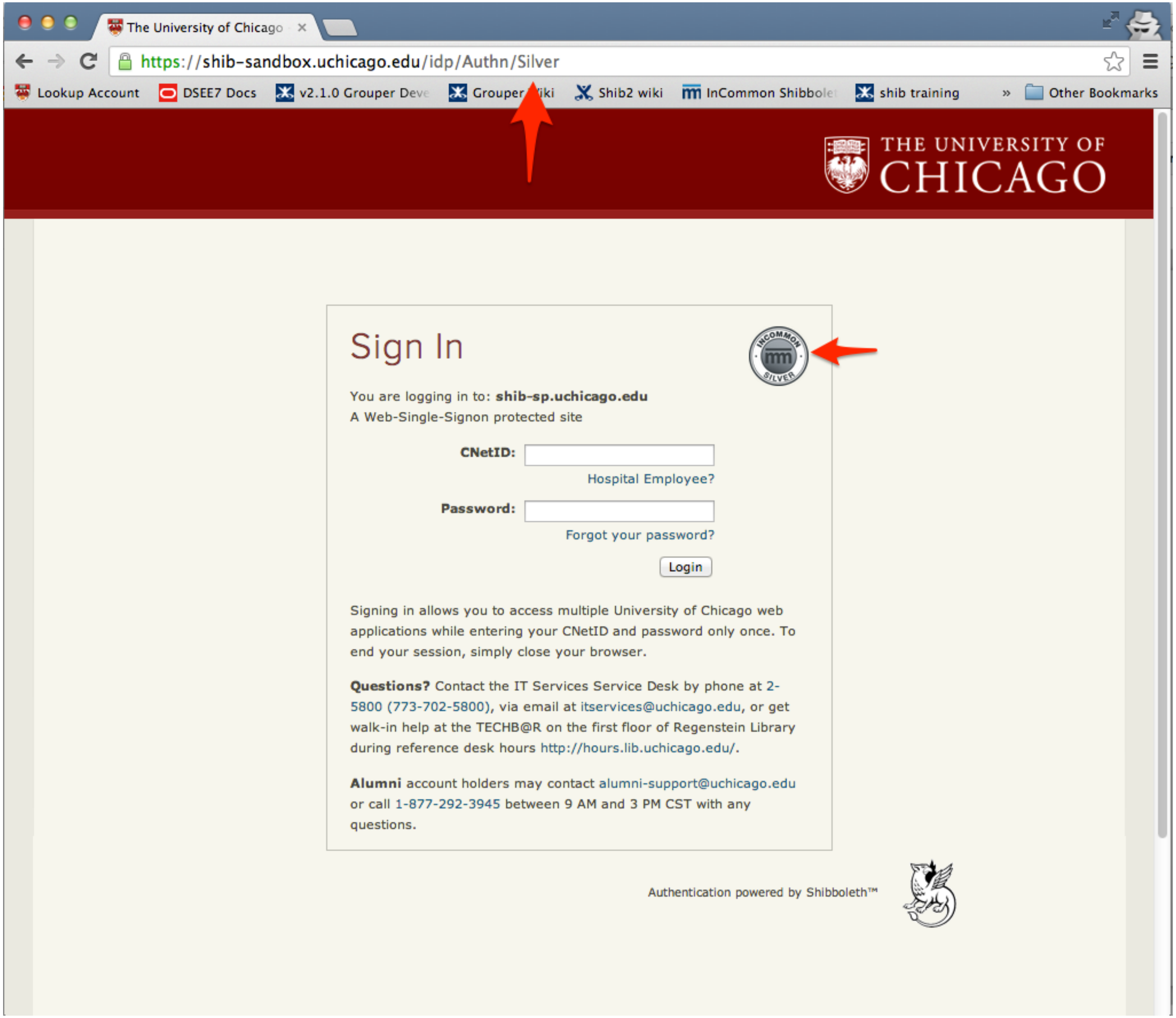
Has Verified Address of Record

Password meets Entropy Requirements

Users who fail AD Audit

Making it work

- Final this-person-can-do-silver group pushed to LDAP
- Shibboleth attribute resolver configured to create attribute eduPersonAssurance based on user being a member of the Silver group
- Custom login handler created which looks at authnContextClassRef and if Silver is requested AND user has eduPersonAssurance Silver then respond positively



Sign In

You are logging in to: **shib-sp.uchicago.edu**
A Web-Single-Signon protected site

CNetID:

Hospital Employee?

Password:

Forgot your password?

Signing in allows you to access multiple University of Chicago web applications while entering your CNetID and password only once. To end your session, simply close your browser.

Questions? Contact the IT Services Service Desk by phone at 2-5800 (773-702-5800), via email at itservices@uchicago.edu, or get walk-in help at the TECHB@R on the first floor of Regenstein Library during reference desk hours http://hours.lib.uchicago.edu/.

Alumni account holders may contact alumni-support@uchicago.edu or call 1-877-292-3945 between 9 AM and 3 PM CST with any questions.

Authentication powered by Shibboleth™

About AD @ Chicago

- Not possible at this time to make AD Silver compliant
- Silver passwords transmitted to AD & stored in AD
- Daily audit process created to monitor authentication events
- NTLMv1 events and unsigned LDAP authentication events trigger compliance process

AD Compliance Process

- User’s caught by the audit process placed in grouper group
- Group-math causes user to lose Silver
- User notified via email and user dashboards that there was a problem & to contact local support
- Support works with Windows Server team to identify & remediate problem
- User changes password & Silver is restored

Future Directions

- Add Bronze support
- Migrate from custom LoginHandler to new Multi-Context Broker being developed by InCommon
- Make 2-Factor an option for Silver AuthN

Thank You

davel@uchicago.edu