Identity Finder Frequently Asked Questions

Privacy/General Questions:

What will Identity Finder search for in my files?

Identity finder has been restricted to search for only the most sensitive data (also known as PII):

- Bank account numbers
- Social Security numbers
- Credit card numbers
- Passport numbers
- Driver's License numbers

Will Identity Finder look through all my documents?

Yes, but it is not scanning for anything other than a very specific set of number sequences formatted in a very specific way. Identity Finder is not reading your documents to find out anything about you other than if there is any personally identifiable information (PII) in the document.

Where is Identity Finder searching?

Identity Finder has been pre-configured to only search the part of your computer that contains user information (i.e. home folders). You will also be able to adjust where Identity Finder searches, including scanning external drives and other parts of your computer's hard disk. The program will not allow you to scan network drives or Exchange email folders.

Will the Identity Finder team be able to see any of the information that the scan finds?

No, the identity finder team will not be able to see any of the numbers that are found on your computer. Team will only see the filenames and folders where the data is contained.

Who will scan my computer?

It is highly recommended the employee initiate the scan to locate restricted and sensitive data. After thirty days of the campus Identity Finder announcement, the system will initiate an automatic scan if the employee has not scanned their computer at least once.

Will Identity Finder report anything illegal it finds on my computer?

No, Identity Finder is only scanning through your documents to find a very specific set of numbers formatted a very specific way. Identity Finder is not looking at the contents of your computer outside of these numbers.

What happens if Identity Finder finds PII on my computer?

Identity Finder will present you, the end user, with a list of every item it thinks is PII at the end of the scan. Ultimately, the user and/or their supervisor will determine if the data is sensitive enough to

warrant removal or if it's a false positive. The Information Security team can advise, as necessary, to either confirm that it is PII and should be removed/scrubbed, or that it is a false positive and can be left alone.

After you have finished cleaning, the Identity Finder client will send some of the data collected back to the Identity Finder team for reporting purposes only. The information stored in the console never includes the sensitive data; it contains information about where sensitive data was found, and what was done about it.

What is Identity Finder sending back to the Identity Finder team?

1. The location on your computer where the file containing PII was found
2. The name of the file
3. The action you took against the PII
4. The date and time it was found
5. The type of PII found (SSN, Credit Card number, Passport, etc.…)
6. The file format that it was found in
7. The number of instances of PII were found in each file

Once PII data is discovered, what actions can be taken?

- Data may be shredded (permanently delete files containing sensitive information)
- Data may be scrubbed (redact sensitive data but leave the rest of the file intact). This only applies for text files, MS Word/Excel/PowerPoint files.
- You can choose to 'ignore' the match found, should you feel it's a false positive and not PII

  Please note: Once you take action on discovered items, these items will no longer be reported in future scans.

Will Identity Finder search my email?

Identity Finder only searches files located on your computer. If you are using email software that downloads and stores your emails on your computer (i.e. .pst files), Identity Finder will scan your emails. Identity Finder ***will not*** search your Exchange email folders located on the Exchange server.

Identity Finder found some of the items that are considered restricted/confidential. What if I need to keep this data on my computer to perform my job?

It's highly recommended the data be moved to a more secure l location on our network file shares, managed by Information Technology. This data is protected by campus firewalls and security access controls on the file share. If this is not possible (for whatever reason), ensure your computer is encrypted. Contact the IT Service desk, and they will assign a work order for to address your task.

Identity Finder Frequently Asked Questions

Technical Questions:

How do I shred a file?

A file can be shredded by selecting the check box next to the file name and clicking on the shred button on the top ribbon. Once a file is shredded, it is permanently erased.

I accidentally shredded a file, how do I get it back?

You cannot retrieve a file that has been shredded. It is deleted in accordance with Department of Defense standards and is effectively irrecoverable.

I would like to have Identity Finder search for more specific information. Is this possible?

Yes, Identity finder does provide the option to search for specific information. For instance, if you wish to search for your phone number or home address, you will be able to do that. The Identity Finder technical team can assist with creating custom search query.

I'm having trouble adjusting some settings in Identity Finder.

Identity finder has been restricted to search for only the most sensitive data:

- Bank account numbers
- Social Security numbers
- Credit card numbers
- Passport numbers
- Driver's License numbers

If you wish to search for any additional values, please see the entry on searching for more specific information.

You will also be able to adjust where Identity Finder searches for data, including external drives and other parts of your computer's hard drive. It will not allow you to scan network drives and Exchange email folders.

If a setting is unable to be changed, and you have a valid reason for it to be configured by the user, contact the IT Service Desk and the Identity Finder team will assess your request and get back to you as soon as possible.

Can I scan my computer at my own request?

Yes, but it is important to review the training documentation first to minimize errors and accidental deletions.

Who can I contact for more information?

Feel free to contact Jim Packard, ACIO & Information Security Officer (james_packard@uml.edu) or send email to infosec@uml.edu.