

Contact Us

Gail McDermott

Director
(617) 496-9948

gail_mcdermott@harvard.edu

Michael Monaghan

Director, Financial, Operational &
Compliance Audit
(617) 496-2165

michael_monaghan@harvard.edu

James Yung

Associate Director, Information Systems Audit
(617) 495-2166

james_yung@harvard.edu

Amanda McDonnell

Manager of Strategic Planning
(617) 496-8980

amanda_mcdonnell@harvard.edu

Insurance Department

(617) 495-7971

<http://fad.harvard.edu/rmas>

Do you have questions or concerns about which you don't feel comfortable speaking to a supervisor or other resource?

Call the University's anonymous, 24-hour Compliance Hotline and speak with a trained communications specialist who is not affiliated with the University. The specialist will send a report to University management for review and, if necessary, investigation.

Compliance Hotline

1-877-694-2ASK
(2275)



Report via the Web:

<https://www.integrity-helpline.com/HarvardUniversity.jsp>

Protecting Your Identity

Risk Management & Audit Services



**Protecting
Your Identity**
Risk Management & Audit Services

Risk Management & Audit Services

1033 Massachusetts Ave., 3rd Floor

Cambridge, MA 02138

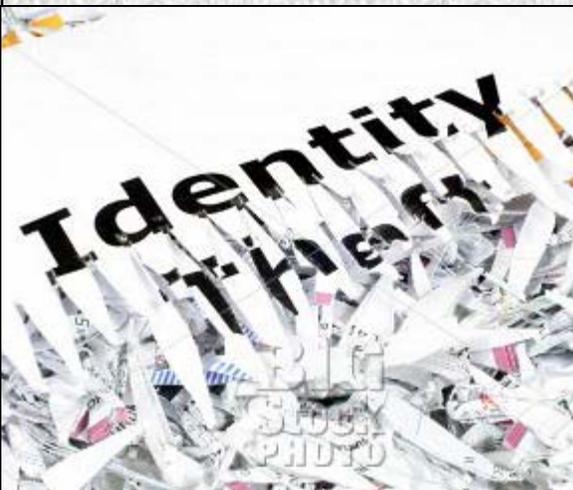
(617) 496-7108

<http://fad.harvard.edu/rmas>



Identity Theft—A Growing Problem

Identity theft is one of the fastest-growing types of crime. Identity theft is the fraudulent use of an individual's unique identifying information and/or personal data. This information includes, but is not limited to, Social Security numbers (SSNs), driver's license numbers, birth certificate and passport information. Victims with high credit ratings are especially lucrative targets for identity thieves since they could take out mortgages, unsecured lines of credit or other large credit instruments.



Identity Theft on a Personal Level

If someone steals your identity, it could:

- Destroy your positive credit rating, causing accounts to be closed and making it impossible to open new accounts.
- Cause problems in obtaining employment, tenancy or other social services.
- Subject you to collection actions and creditors seeking remuneration for fraudulent accounts opened in your name.
- Cost you thousands of dollars and take years to resolve.
- Subject you to possible arrest, interrogation and detention by law enforcement acting on information about a criminal who assumed your identity.

Working with Personal Identifiable Information

Harvard University classifies personal identifiable information as “High Risk Confidential Information” (HRCI). HRCI is protected by Massachusetts law. Improper use or disclosure of the information is subject to regulatory reporting. For more information on Harvard policy, visit www.security.harvard.edu or you have any questions contact security@harvard.edu.

Steps to protect HRCI:

- **Destroy unneeded documentation or media containing HRCI.** Shredding should take place regularly for documents containing HRCI that are no longer needed or required. For media devices, information should be removed using a secure erasure application or destroy the media.
- **Protect electronic data.** Personal data stored in databases needs to be safeguarded. Harvard employees working with HRCI must use a Harvard issued and managed computer with disk encryption installed.
- **Safeguard non-electronic or paper documents.** Documents containing HRCI must be locked in a file cabinet when not in use.
- **Test the vulnerability of computer databases.** Targeted systems containing HRCI should be scanned periodically for security vulnerabilities.
- **Use secure passwords and do not share the passwords.**