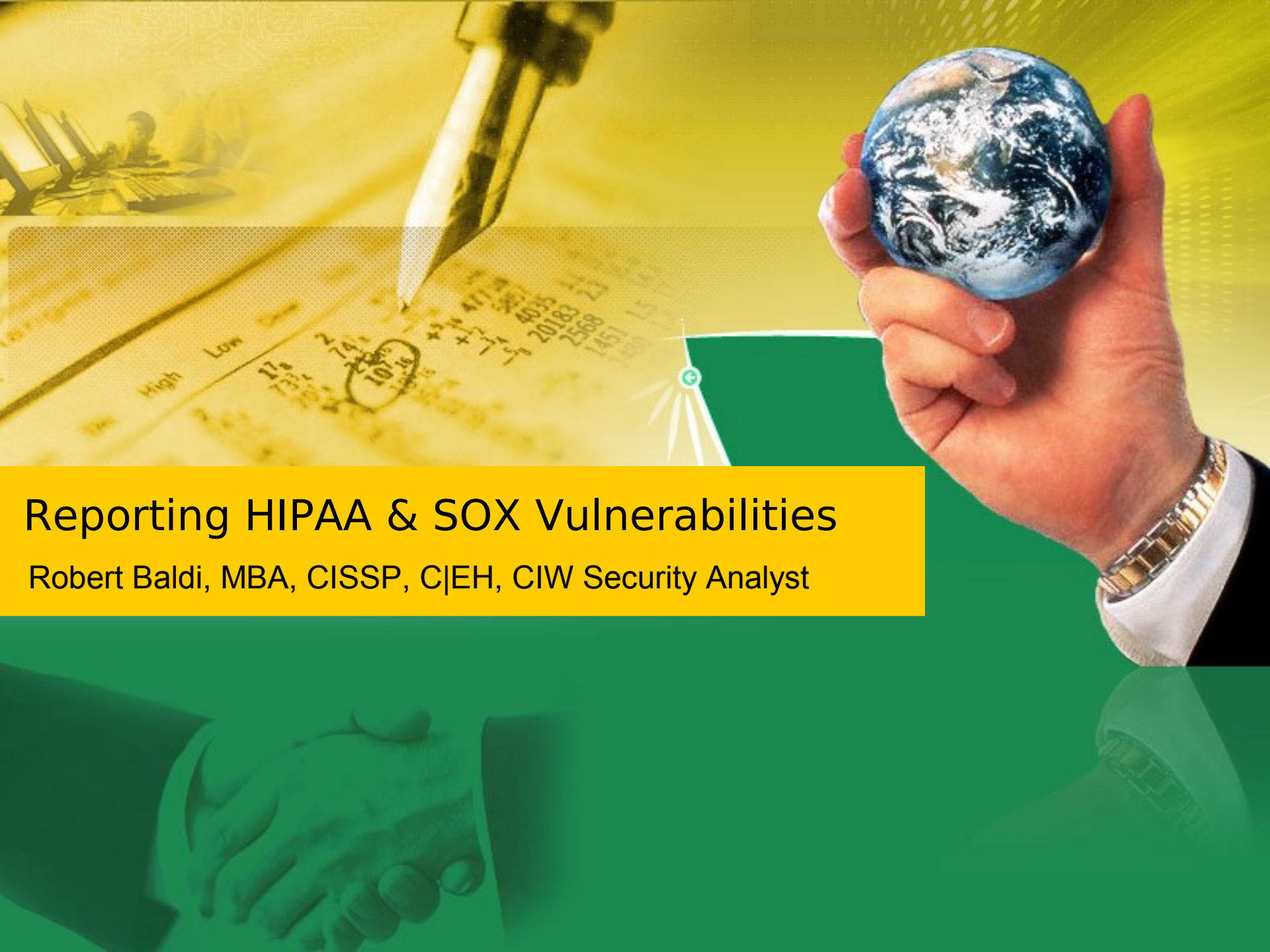


Reporting HIPAA & SOX Vulnerabilities

Robert Baldi, MBA, CISSP, C|EH, CIW Security Analyst

Overview

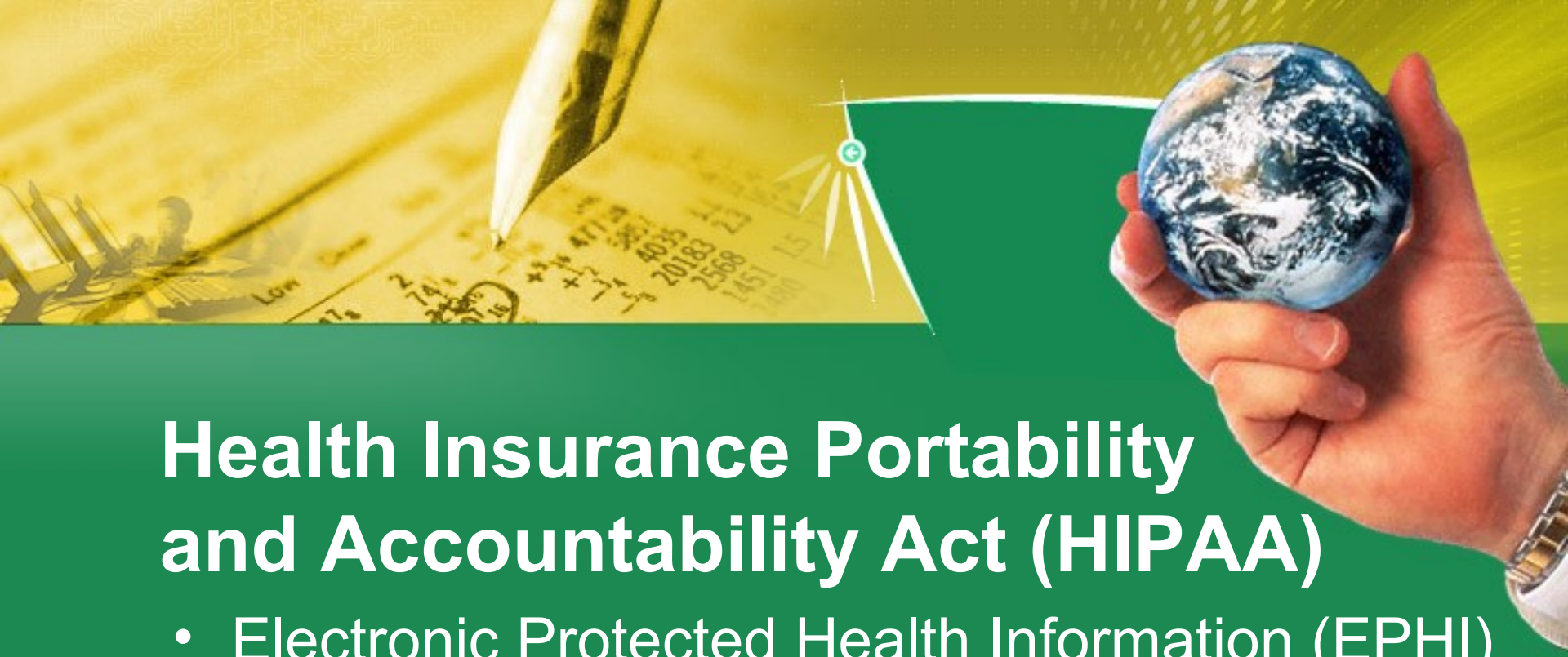
- Understanding the vulnerability reporting problem
- Reporting vulnerabilities
- Overview of HIPAA
- Overview of SOX security requirements
- How to report HIPPA & SOX vulnerabilities
- Review

Understanding the problem

- "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.“
  - **Bruce Schneier**

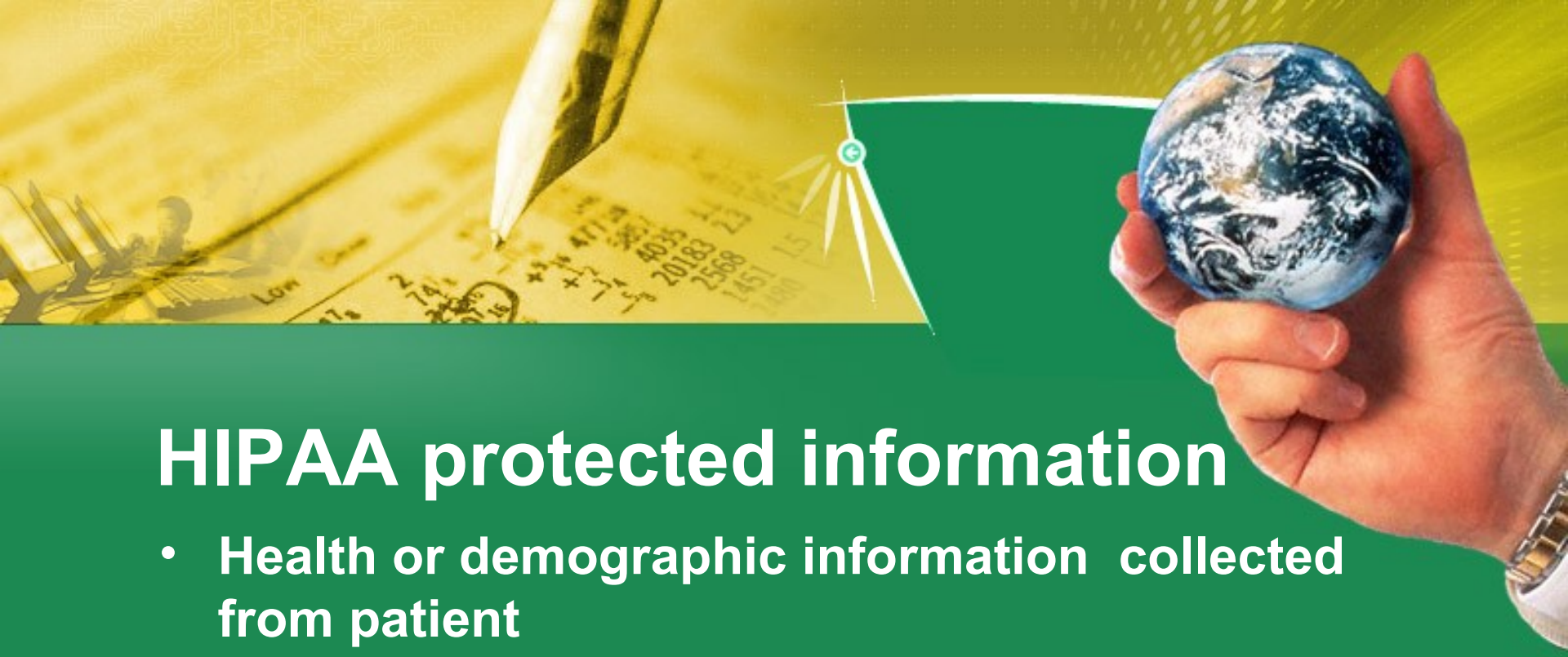
Reporting vulnerabilities

- Helps protect other organizations
  - **Limits attackers targets**
- Required by laws (HIPAA, SOX, State)
  - **Executives/employees can face jail/fines**
  - **Fair Credit Reporting Act**
- Negative Publicity
- Loss of consumers
- Loss of business partners
- Legal liability



Health Insurance Portability and Accountability Act (HIPAA)

- Electronic Protected Health Information (EPHI)
  - **Administrative Safeguards**
  - **Physical Safeguards**
  - **Technical Safeguards**
  - **Documentation Standard**



HIPAA protected information

- Health or demographic information collected from patient
- Created or received by covered entity
- Information related to an individual's past, present or future physical or mental health of patient and related treatment and payment functions
- If there is a reasonable basis to believe the information can be used to identify the patient

HIPPA VIOLATION EXAMPLES

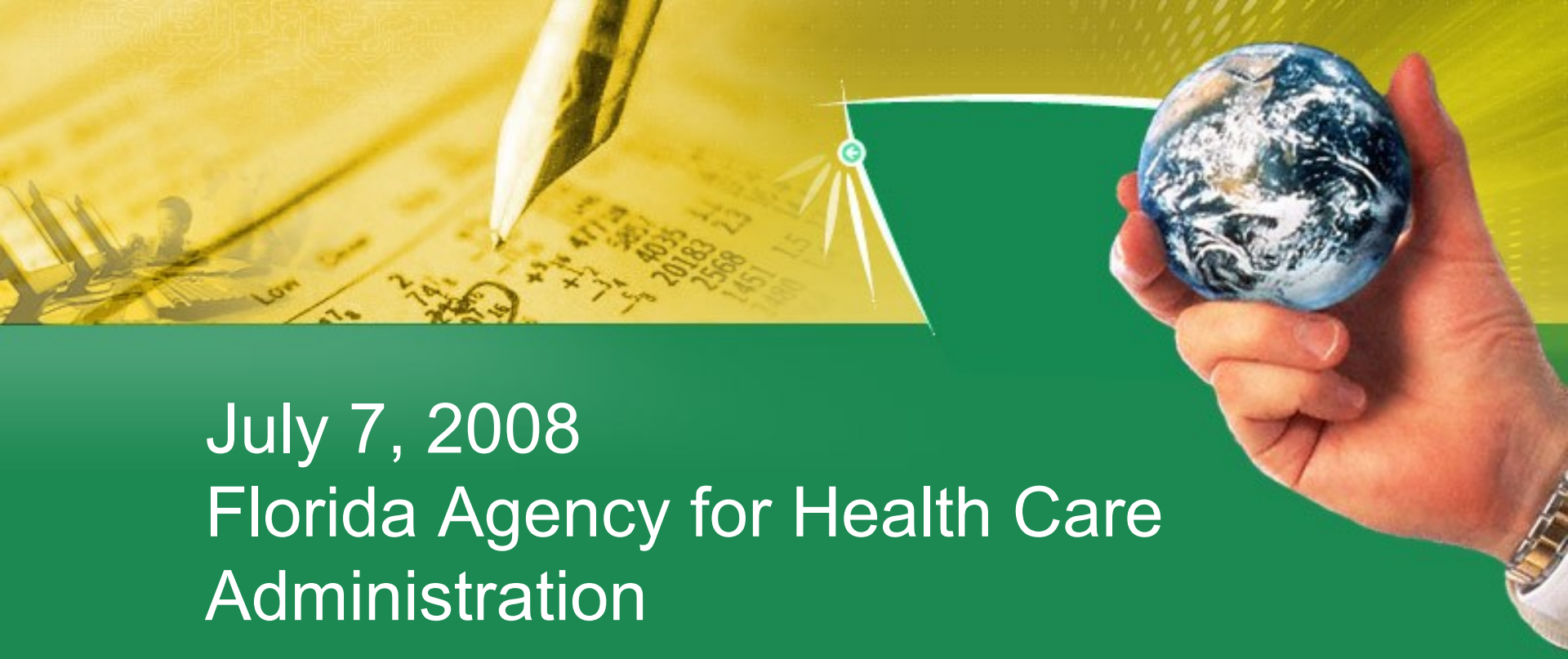
http://www.privacyrights.org

June 11, 2008
U-Utah Data Breach Hits 2.2 Million

(Greensboro, NC) billing tapes were stolen from the personal car of a driver at Perpetual Storage, a local company that for 16 years has stored the university's tapes in an off-site vault. The driver violated company protocols by not using a secure company van and leaving the tapes in his car overnight instead of delivering them to the vault.

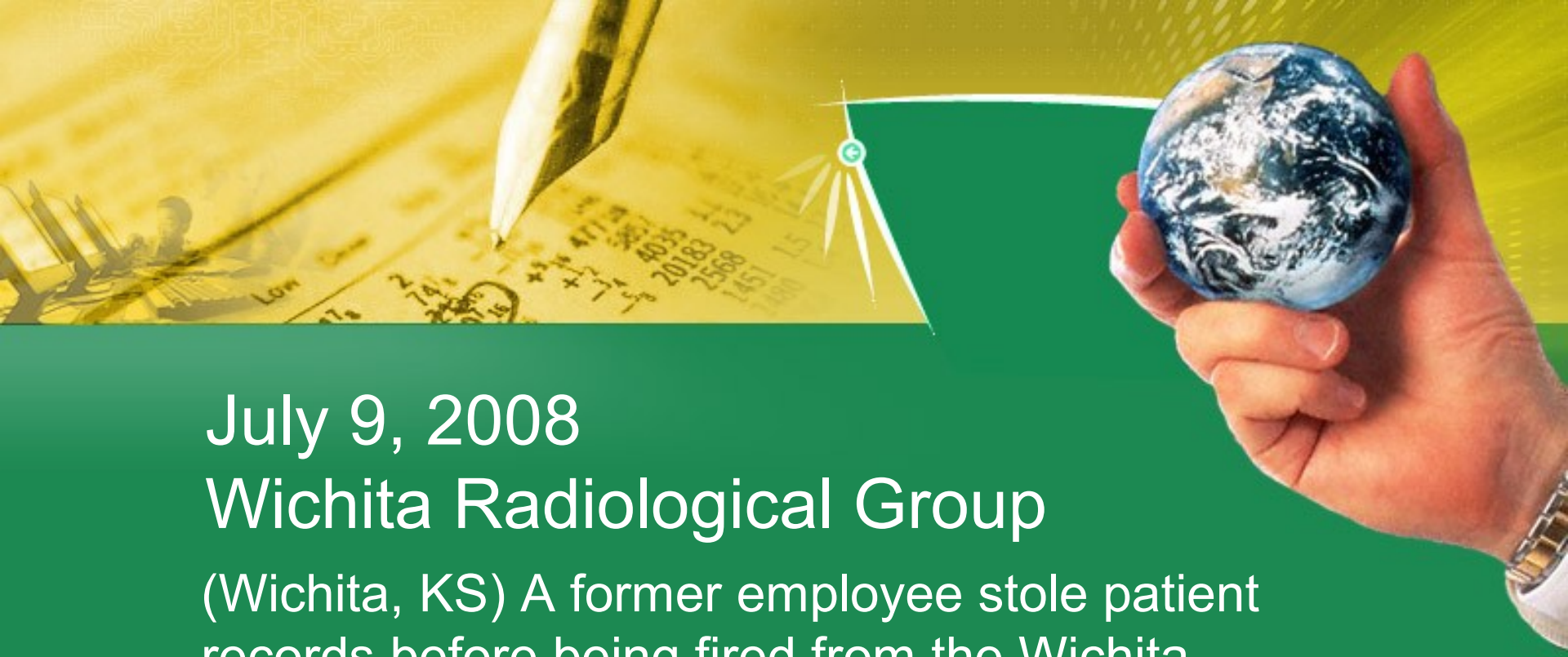
July 2, 2008
Baptist Health

(Little Rock, AR) Due to a breach by an unauthorized person in the information systems, there is a possibility that some personal information, such as name, address, date of birth, Social Security number, and reason for coming to Baptist Health. No information in the patient's "medical records" and no information about the patient's diagnosis or prognosis was accessed. 1,800 patients impacted.



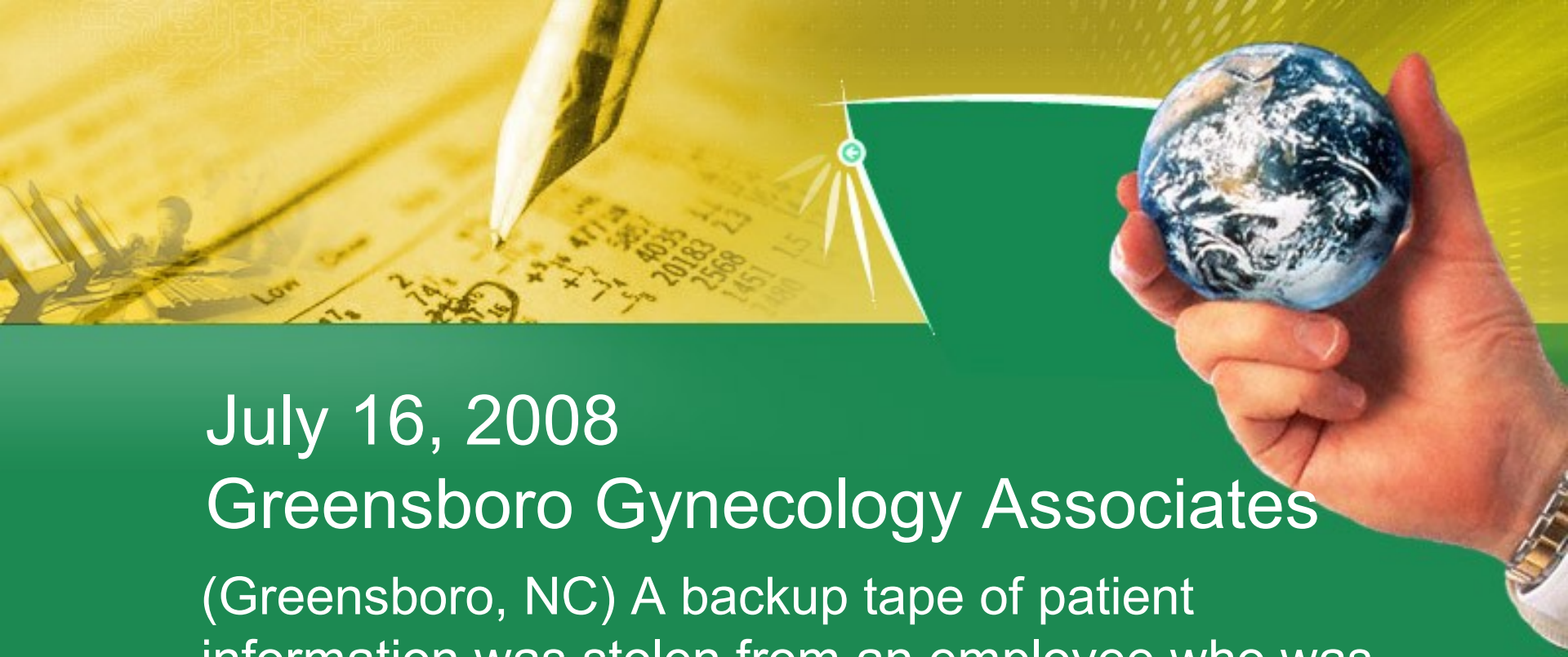
July 7, 2008
Florida Agency for Health Care Administration

(Tallahassee, FL)A security breach in the Organ and Tissue Donor Registry may have exposed thousands of donors' personal information, including their Social Security numbers. Other data included donors' names, addresses, birth dates and driver license numbers. 55,000 patients impacted.



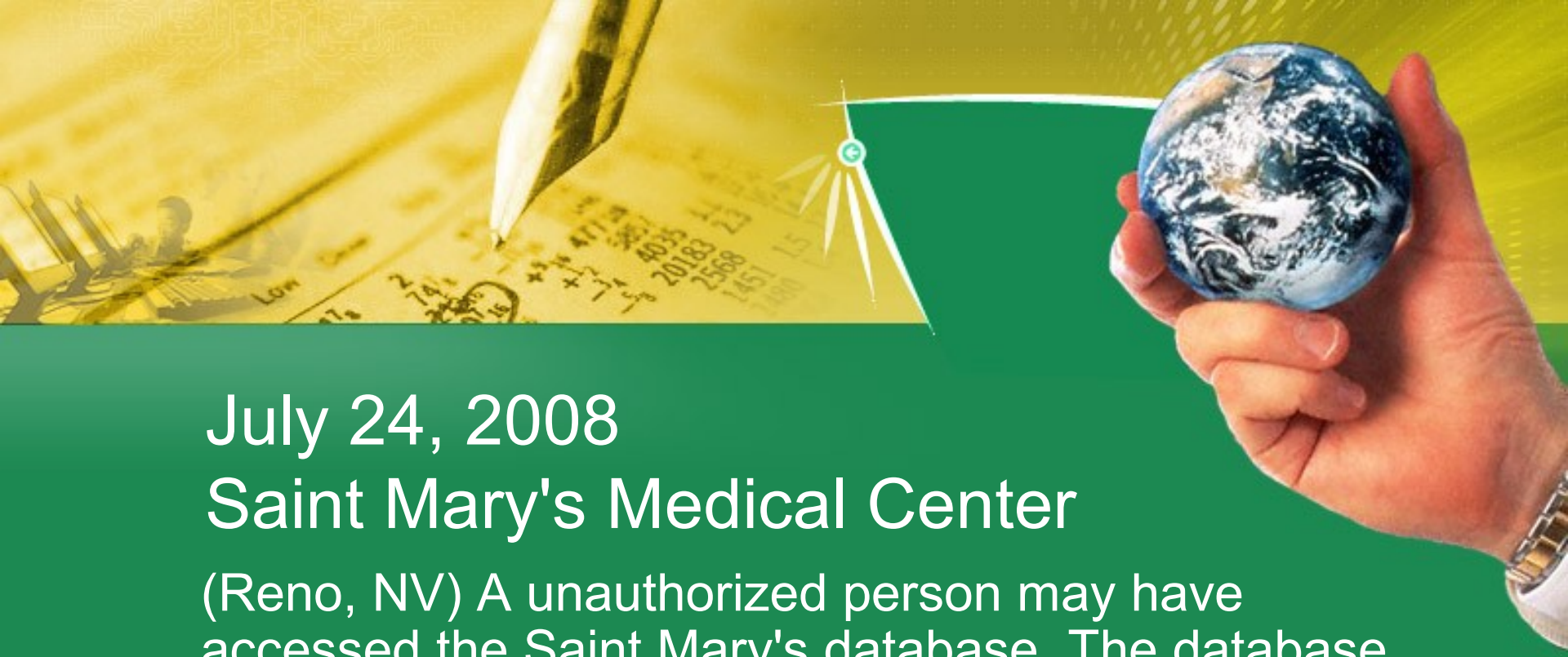
July 9, 2008
Wichita Radiological Group

(Wichita, KS) A former employee stole patient records before being fired from the Wichita Radiological Group. Tens of thousands of patient records were in the database could have been compromised.



July 16, 2008
Greensboro Gynecology Associates

(Greensboro, NC) A backup tape of patient information was stolen from an employee who was taking the tape to an off-site storage facility for safekeeping. The stolen information included patients' names, addresses, Social Security numbers, employers, insurance companies, policy numbers and family members. 47,000 patients impacted.



July 24, 2008
Saint Mary's Medical Center

(Reno, NV) A unauthorized person may have accessed the Saint Mary's database. The database, used for Saint Mary's health education classes and wellness programs, contained personal information such as names and addresses, limited health information and some Social Security numbers. The database did not contain medical records or credit card information. 128,000 patients impacted.

July 25, 2008
Grady Memorial Hospital

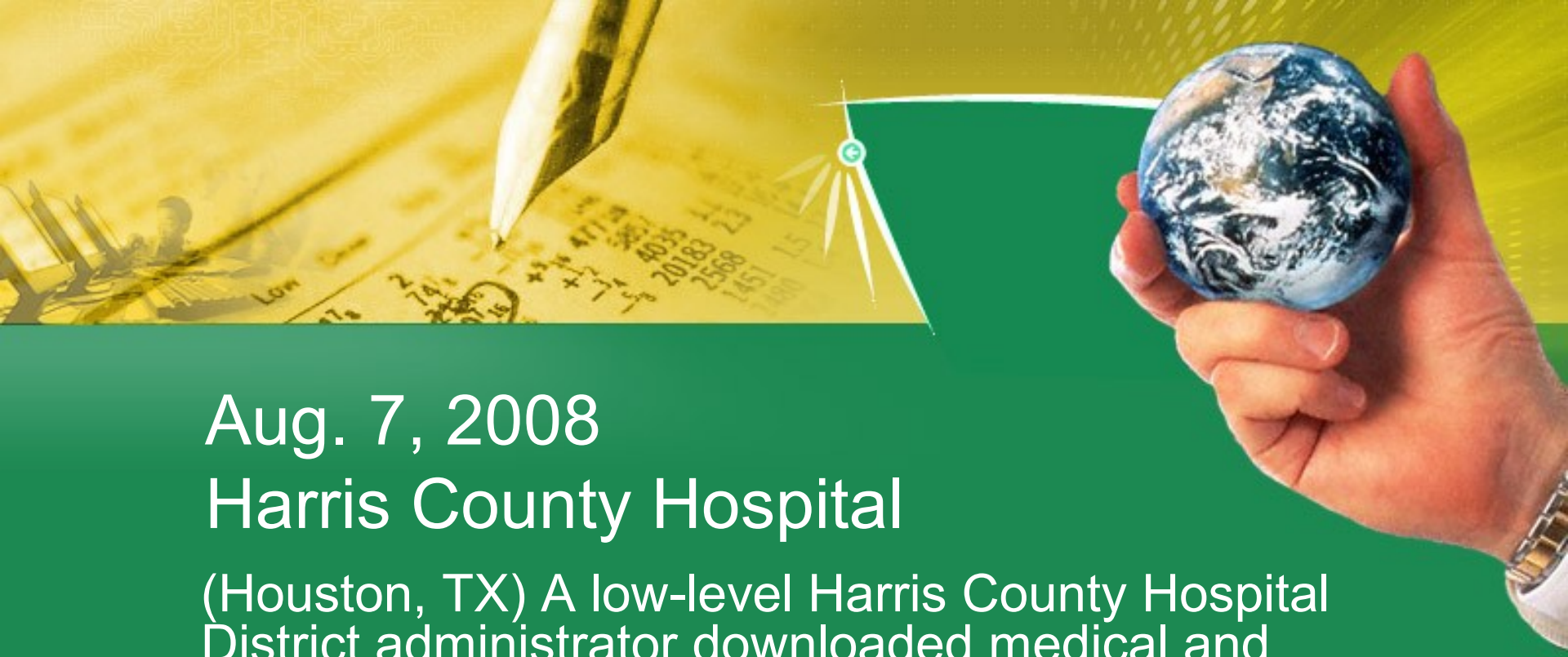
(Atlanta, GA) Hospital records were stolen. It remains unknown how many patient records were stolen, which patients were affected or how the records were stolen. The records pertained to recorded physician comments that Grady sent to a vendor to transcribe into medical notes. The records were stolen from a subcontractor employed by the vendor. Unknown number of patients impacted.

July 25, 2008
Indianapolis Hospital Data Breach

(Indianapolis, IN) St. Vincent Indianapolis Hospital announced that about 51,000 patients' personal data, including names, addresses and Social Security numbers, in the spring were made publicly available on the Internet due to a security lapse by a subcontractor, the Indianapolis Star reports. 51,000 patients impacted.

July 29, 2008
Blue Cross Blue Shield

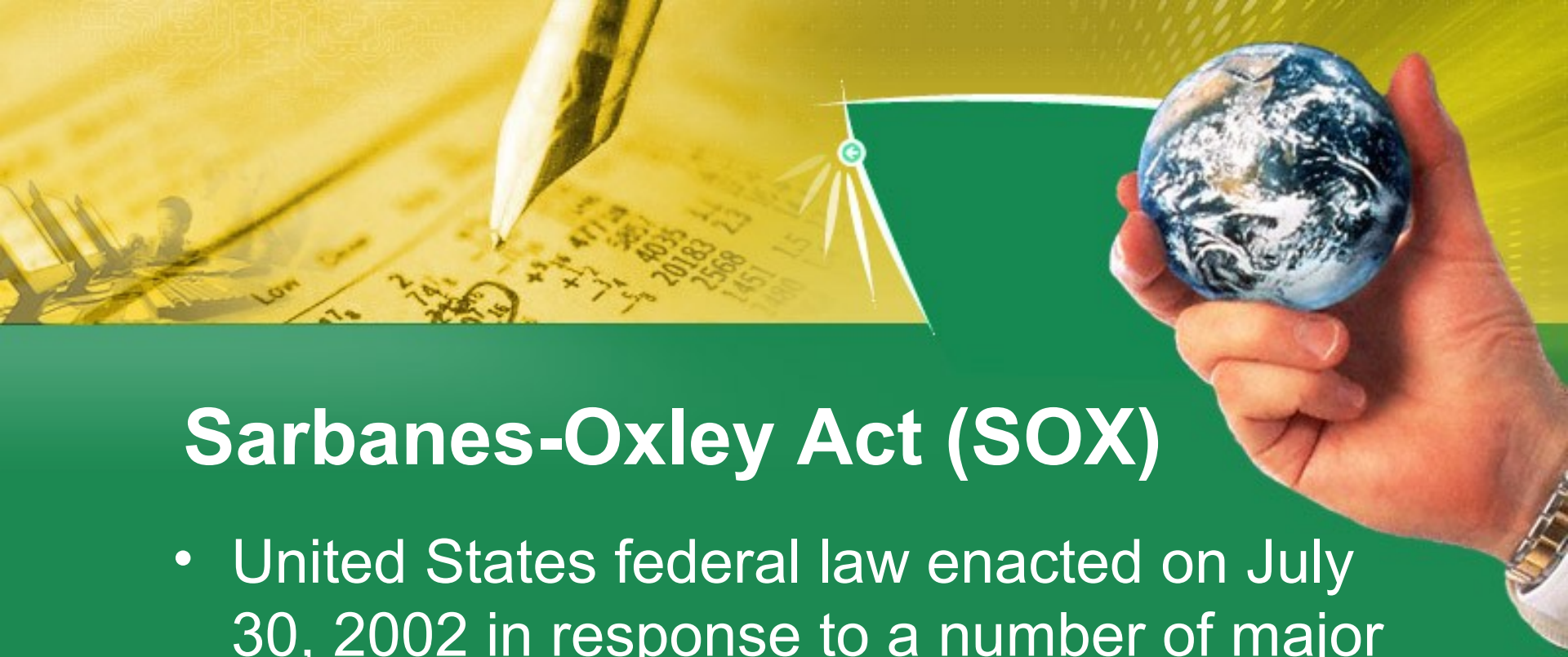
(Atlanta, GA) Letters containing personal and health information were sent to the wrong addresses last week. The letters included the patient's name and ID number, the name of the medical provider delivering the service, and the amounts charged and owed. A small percentage of letters also contained the patient's Social Security numbers. 202,000 patients impacted.



Aug. 7, 2008
Harris County Hospital

(Houston, TX) A low-level Harris County Hospital District administrator downloaded medical and financial records for patients with HIV, AIDS and other medical conditions onto a flash drive that later was lost or stolen. The data on the device included the patients' names, medical record numbers, billing codes, the facilities where the office visits occurred and other billing information. It also included the patients' Medicaid or Medicare numbers, which can indicate their Social Security numbers or those of their spouses. 1,200 patients impacted.


WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
AK
HI
51K
47K
128K
202K
2.2M
55K
1.8K
1.2K
2,686,000 records stolen



Sarbanes-Oxley Act (SOX)

- United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals
- Falls under the umbrella of the U.S. Securities and Exchange Commission
- Applies to all U.S. public companies
- Section 404 – Information Technology

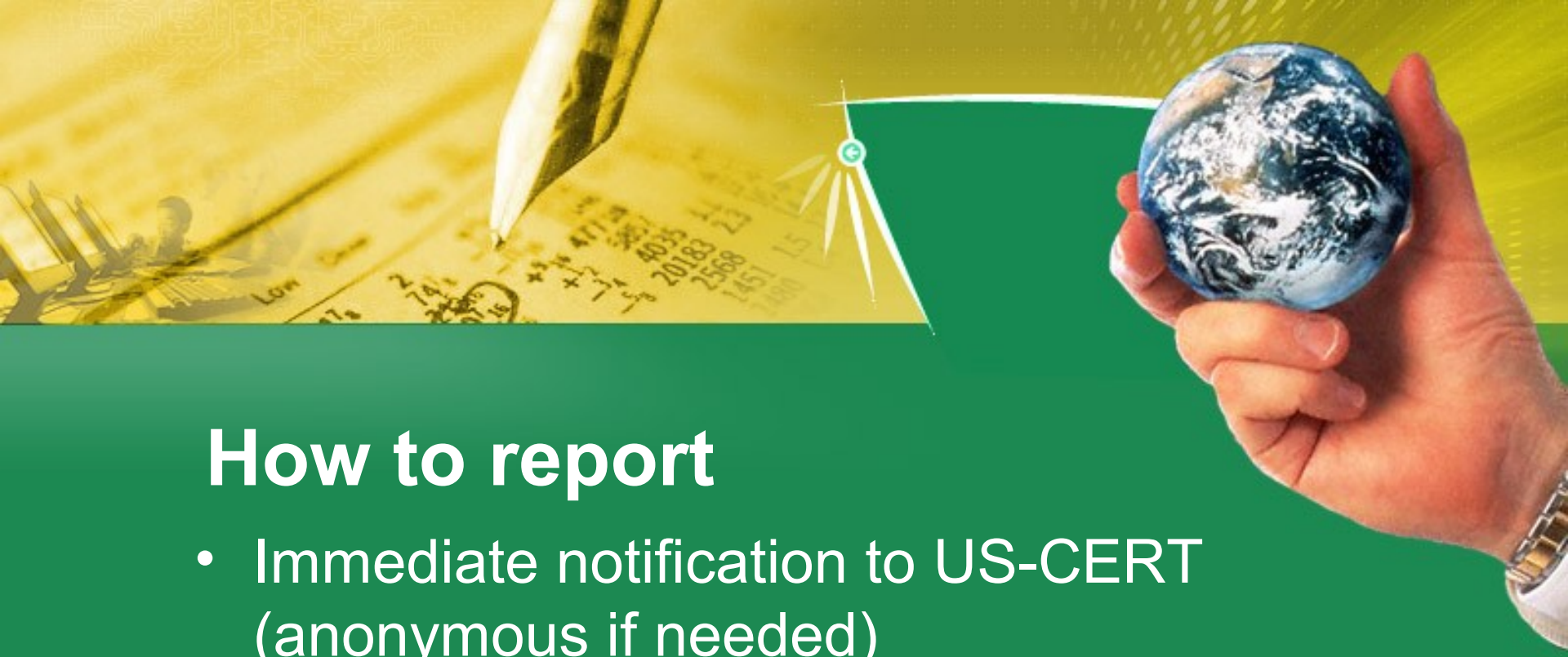
http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf

SOX VIOLATION EXAMPLES

http://www.privacyrights.org

SOX violations past 90 days

- Wells Fargo, 5,000 impacted
- Countrywide Financial, 2,000,000 impacted
- Anheuser-Busch, unknown
- Facebook, 80,000,000 impacted
- Citibank, unknown
- Domino's Pizza, unknown
- ATT/Cingular, unknown



How to report

- Immediate notification to US-CERT (anonymous if needed)
- Notify key personnel within your organization
  - **Prepare public relations material**
- After the incident response and isolation, determine clientele impacted
  - **Send mail to all customers disclosing exactly what happened and how you addressed it**

Review

- Understand the vulnerability reporting problem
- What HIPAA violations need to be reported
- What SOX violations need to be reported
- How to report HIPPA & SOX vulnerabilities

Questions