SQUIRE SANDERS

STROZ FRIEDBERG

What Keeps You Up at Night?

Issues of Fraud and Abuse Compliance Series

My Data's Been Stolen: Now What?
Part I

September 19, 2013

39 Offices in 19 Countries

SQUIRE SANDERS

STROZ FRIEDBERG

The Washington Post

After a year-long study of cybersecurity, the Washington Post concluded that healthcare companies are among the most vulnerable in the U.S.

Source: "Health-care sector vulnerable to hackers, researchers say," Washington Post (December 25, 2012)

SQUIRE SANDERS

STROZ FRIEDBERG

"I have never seen an industry with more gaping security holes.

"If our financial industry regarded security the way the healthcare sector does, I would stuff my cash in a mattress under my bed."

Avi Rubin, a computer scientist and technical director of the Information Security Institute at Johns Hopkins University.

"Health-care sector vulnerable to hackers, researchers say," Washington Post (December 25, 2012)

SQUIRE SANDERS

STROZ FRIEDBERG

Today's Hosts

Thomas E. Zeno
Of Counsel, Squire Sanders
T +1 513 361 1202
thomas.zeno@squiresanders.com

Emily E. Root
Senior Associate, Squire Sanders
T +1 614 365 2803
emily.root@squiresanders.com

SQUIRE SANDERS

STROZ FRIEDBERG

Today's Speakers

Scott A. Edelstein
Partner, Squire Sanders
T +1 202 626 6602
scott.edelstein@squiresanders.com

Thomas J. Hibarger
Managing Director, Stroz Friedberg
T +1 202 464 5803
thibarger@strozfriedberg.com

Justin Root
Special Agent – Cyber Crimes Unit
Office of Ohio Attorney General Mike DeWine
T +1 740 845 2080
justin.root@ohioattorneygeneral.gov

SQUIRE SANDERS

STROZ FRIEDBERG

Today's Agenda

- How to know a breach has occurred
- Insider and outsider threats
- Should you notify law enforcement?
- What does HIPAA require about Business Associates?

Part II – November 21, 2013

- What more does HIPAA require?
- Data breach remediation
- Tips to prevent a breach and pre-planning for a breach

SQUIRE SANDERS

STROZ FRIEDBERG

Big-Picture Trends in the World of Hacking

- Increasingly sophisticated tools available for hackers
- Robust underground market for hacker tools and services, as well as stolen information and compromised computers
- Less technical skill is required to pull off sophisticated attacks
- Increased automation of hacking techniques has made it profitable to go after smaller targets – who often have weaker security

SQUIRE SANDERS

STROZ FRIEDBERG

Sample Ads from the Underground

"Programming service; Perl, PHP, C, Java, etc. Prices: From US$100; injects writing: From US$200; web server hacking: From US$250"

"Writing and selling Trojans and other malware; available: Trojan for bank account stealing–US$1,300, Trojan for web page data replacement in a client's browser–US$850, WebMoney Keeper Trojan–US$450, DDoS bot–US$350, credit card checker–US$70, backdoor–US$400, LiveJournal spammer–US$70, fakes of different programs–US$15-25"

"Spider Keylogger Pro v. 1.2.4. FUD 100%. Price: US$50."

"Trojan (steals passwords from Opera, Mozilla Firefox, Chrome, Safari, Mail.ru agent, qip). Price: US$8."

"Backdoor for sale (software for remote access to computers); price: US$25; price of source code: US$50."

"Keylogger Detective 2.3.2 (Trojan with hidden installation); price: US$3."

"Trojan emulates WebMoney Keeper Classic; price: US$500."

Source: Trend Micro, "Russian Underground 101": http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

SQUIRE SANDERS

STROZ FRIEDBERG

Healthcare Data Breach Statistics

94% of Healthcare Organizations surveyed had at least one Data Breach in the last two years

- 33% had between 2 – 5 data breaches in the past 2 years
- 45% had more than 5 breaches in past 2 years (up from 29% in 2010)
- Only 6% reported no data breach

$2.4 million = Average Financial Impact

- Up more than 15% from 2010

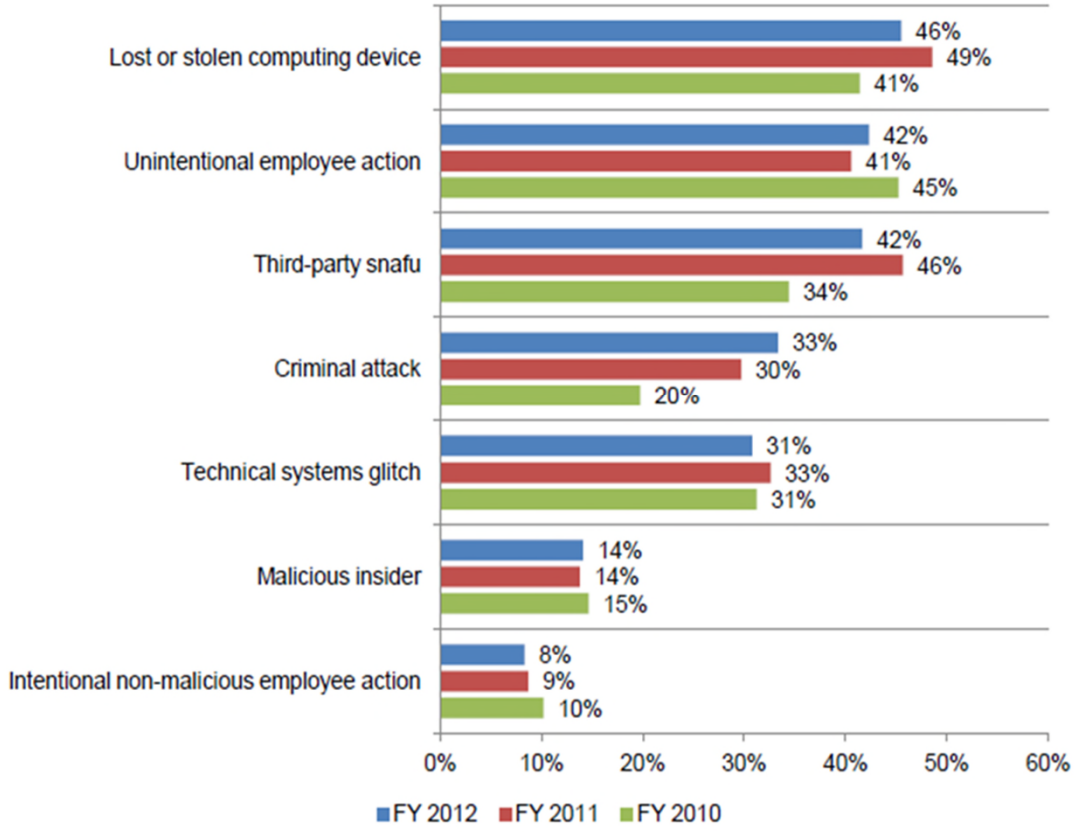
Source: Ponemon Institute© Research Report, Third Annual Benchmark Study on Patient Privacy & Data Security; Dec. 2012

SQUIRE SANDERS

STROZ FRIEDBERG

Healthcare Data Breach Statistics

Figure 5. Nature of the incident
More than one choice permitted



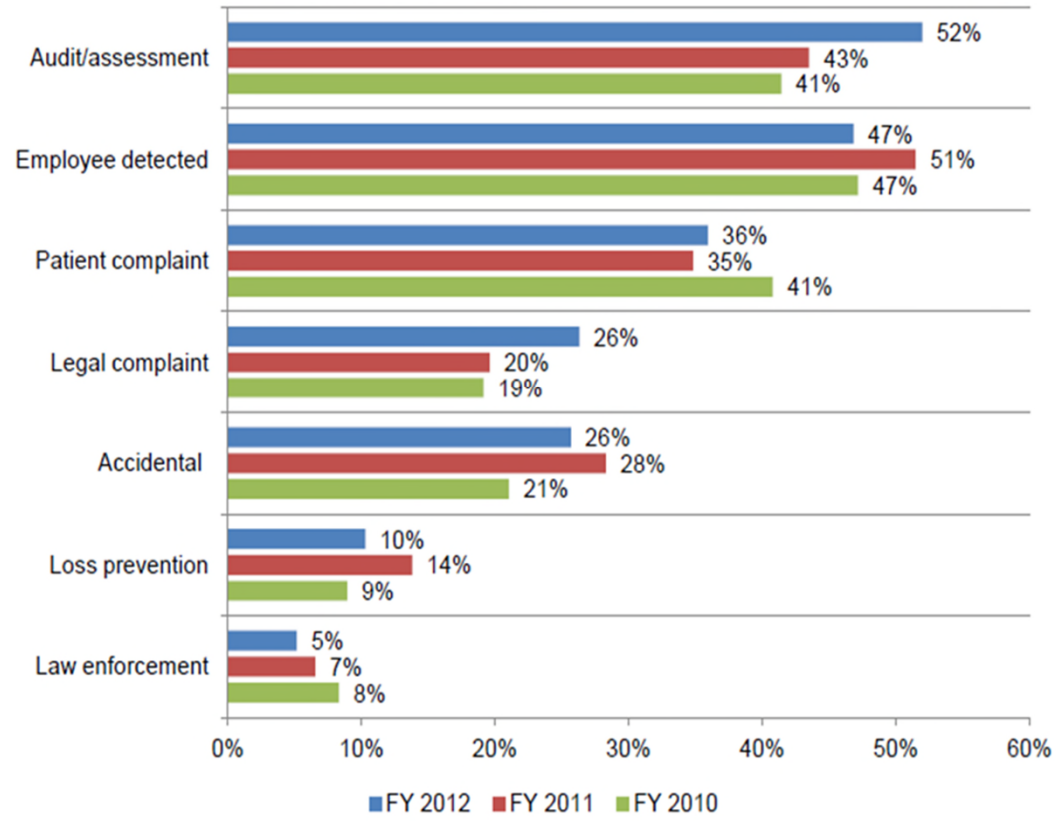
Source: Ponemon Institute© Research Report, Third Annual Benchmark Study on Patient Privacy & Data Security; Dec. 2012

SQUIRE SANDERS

STROZ FRIEDBERG

Healthcare Data Breach Statistics

Figure 7. How the data breach was discovered



Source: Ponemon Institute© Research Report, Third Annual Benchmark Study on Patient Privacy & Data Security; Dec. 2012

SQUIRE SANDERS

STROZ FRIEDBERG

Data Breach - Types

Outsider Threats

- Hacking
  - Phishing/spear phishing
  - Brute force attack
  - SQL injection
  - Advanced Persistent Threat (APT)
  - Hacktivists
- Data theft
  - Media stolen (e.g. laptops, thumb drives, tapes)

SQUIRE SANDERS

STROZ FRIEDBERG

Data Breach - Types

From: **Express Mail Service <el-915@baltimore.com>** Hide
Subject: Tracking Number (N)GHF45 213 213 2126 2126
Date: January 11, 2013 10:10:36 AM EST
To: [redacted]
Reply-To: [redacted]@baltimore.com>

Fed Ex

Order: JN-5584-49069383
Order Date: Thursday, 3 January 2013, 11:23 AM

Dear Customer,

Your parcel has arrived at the post office at January 6.Our courier was unable to deliver the parcel to you.

To receive your parcel, please, go to the nearest office and show this receipt.

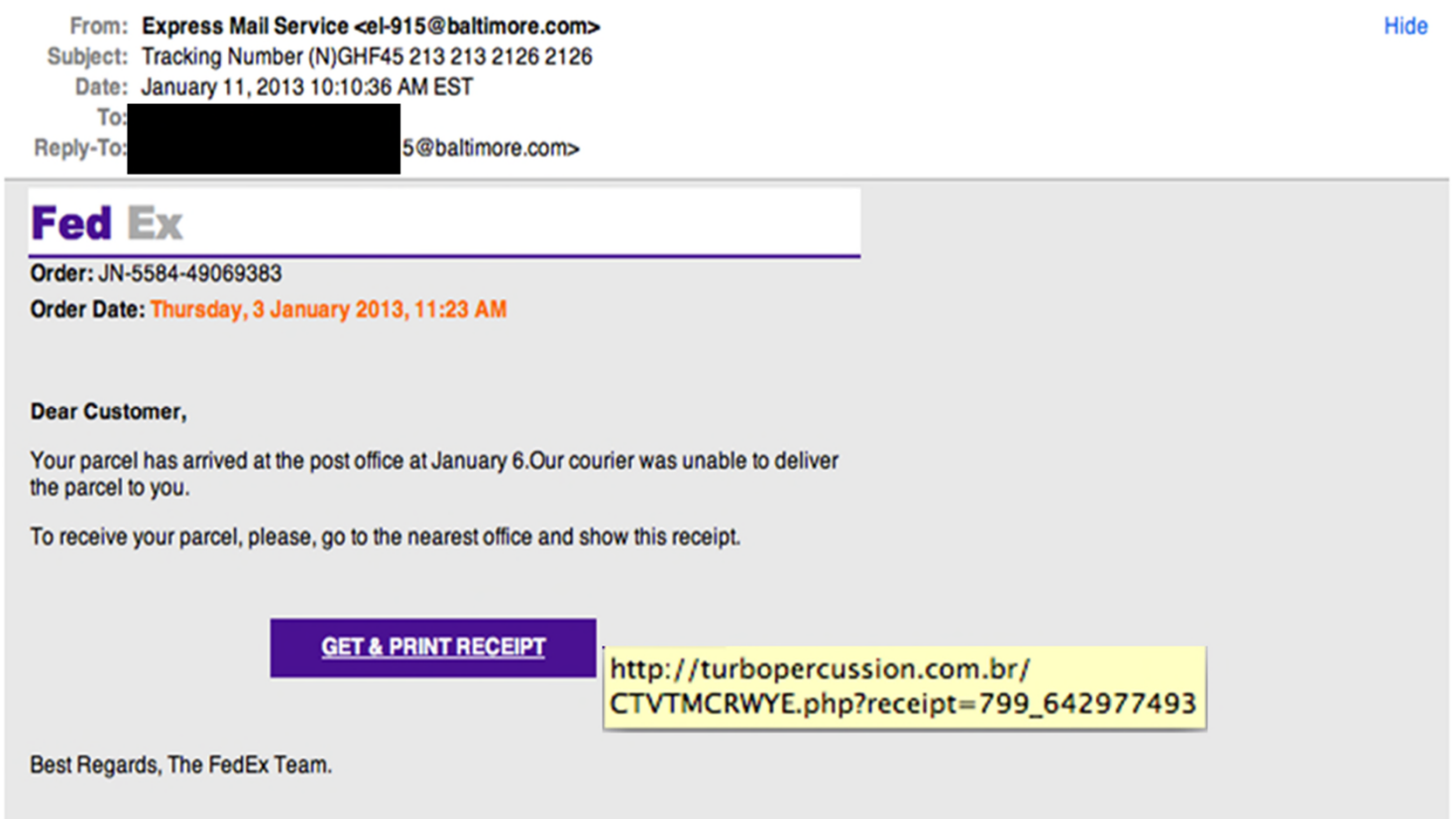
GET & PRINT RECEIPT

Best Regards, The FedEx Team.

SQUIRE SANDERS

STROZ FRIEDBERG

Data Breach - Types



From: **Express Mail Service <el-915@baltimore.com>** Hide
Subject: Tracking Number (N)GHF45 213 213 2126 2126
Date: January 11, 2013 10:10:36 AM EST
To: [redacted]
Reply-To: [redacted]5@baltimore.com>

Fed Ex

Order: JN-5584-49069383
Order Date: Thursday, 3 January 2013, 11:23 AM

Dear Customer,

Your parcel has arrived at the post office at January 6.Our courier was unable to deliver the parcel to you.

To receive your parcel, please, go to the nearest office and show this receipt.

GET & PRINT RECEIPT http://turbopercussion.com.br/CTVTMCRWYE.php?receipt=799_642977493

Best Regards, The FedEx Team.

SQUIRE SANDERS

STROZ FRIEDBERG

Data Breach - Types

From: Thomas Hibarger
Sent: Thursday, August 08, 2013 11:17 AM
To: 'Zeno, Thomas E.'
Cc: Edelstein, Scott A.
Subject: RE: September webinar

Hi Tom & Scott,

Check out these slides for our webinar on 9/19:

www.strozfriedberg.com/webinar

Best,

Tom

Thomas J. Hibarger
Managing Director

STROZ FRIEDBERG
1150 Connecticut Avenue, NW, Suite 700, Washington DC, 20036

SQUIRE SANDERS

STROZ FRIEDBERG

Data Breach - Types

From: Thomas Hibarger badguy@gmail.com
Sent: Thursday, August 08, 2013 11:17 AM
To: 'Zeno, Thomas E.'
Cc: Edelstein, Scott A.
Subject: RE: September webinar

Hi Tom & Scott,

Check out these slides for our webinar on 9/19:

www.strozfriedberg.com/webinar

Best,

Tom

Thomas J. Hibarger
Managing Director

STROZ FRIEDBERG
1150 Connecticut Avenue, NW, Suite 700, Washington DC, 20036

SQUIRE SANDERS

STROZ FRIEDBERG

Data Breach - Types

From: Thomas Hibarger badguy@gmail.com
Sent: Thursday, August 08, 2013 11:17 AM
To: 'Zeno, Thomas E.'
Cc: Edelstein, Scott A.
Subject: RE: September webinar

Hi Tom & Scott,

Check out these slides for our webinar on 9/19:

www.strozfriedberg.com/webinar

Best, www.badguyproxy.ru

Tom

Thomas J. Hibarger
Managing Director

STROZ FRIEDBERG
1150 Connecticut Avenue, NW, Suite 700, Washington DC, 20036

SQUIRE SANDERS

STROZ FRIEDBERG

Data Breach - Types

Insider Threats

- Data theft or loss
  - Data stolen (e.g. by current/former employee = intentional)
  - Data lost (e.g. in taxi = inadvertent)
- Data leakage
  - Exposure to public (e.g. via web site)
  - Exposure to unauthorized person (e.g. wrong employee)
  - Sensitive data sent via unencrypted channel

SQUIRE SANDERS

STROZ FRIEDBERG

Enforcement Trends

- 674 breaches involving 500 or more individuals reported to HHS since 2009
- State Attorneys General become more engaged (e.g, HealthNet)
- DOJ - Dr. Zhou

SQUIRE SANDERS

STROZ FRIEDBERG

Enforcement Trends

- HHS - Office of Civil Rights
  - Wellpoint - $1.7 million settlement - 2013
  - Hospice of North Idaho settlement Dec. 2012
    - Paid $50,000; 441 patients; unencrypted laptop computer stolen June 2010
    - No policies or procedures to address mobile device security as required by HIPAA
    - "Encryption is an easy method for making lost information unusable, unreadable and undecipherable"
- HHS initiative
  - *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information*
    - *Learn more at* www.HealthIT.gov/mobiledevices

SQUIRE SANDERS

STROZ FRIEDBERG

Internal Breaches

Law Enforcement

- Should you report to law enforcement?
- What to expect from law enforcement

SQUIRE SANDERS

STROZ FRIEDBERG

Should You Report to Law Enforcement?

- You may be obligated:

  Ohio Rev. Code § 2921.22(A)(2): No person, knowing that a violation of division (B) of section 2913.04 of the Revised Code has been, or is being committed or that the person has received information derived from such a violation, *shall knowingly fail to report the violation to law enforcement authorities.*

  - Second Degree Misdemeanor
  - Up to 90 days in jail and maximum $750 fine

SQUIRE SANDERS

STROZ FRIEDBERG

Should You Report to Law Enforcement?

Ohio Rev. Code § 2913.04(B): No person, in any manner and by any means, including, but not limited to, computer hacking, shall knowingly gain access to…any computer…without the consent of…the owner of the computer….

- Felony (5th through 2nd degree)

SQUIRE SANDERS

STROZ FRIEDBERG

Should You Report to Law Enforcement?

- You may want to do so:

  Ohio Rev. Code § 1349.19:

  - (B)(1), (2), (C): [Requires notification of a "breach of the security of the system" to anyone whose PII has been accessed if the access creates a "material risk of identity theft or fraud."]
  - (G): [Requires notification consumer reporting agencies of a breach requiring disclosure to more than one thousand residents of the state.]

SQUIRE SANDERS

STROZ FRIEDBERG

Should You Report to Law Enforcement?

- You may want to do so:

Ohio Rev. Code § 1349.19:

- (D): "The person **may delay the disclosure** or notification required by division (B), (C), or (G) of this section **if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation** or jeopardize homeland or national security, in which case, the person **shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation** or jeopardize homeland or national security."

SQUIRE SANDERS

STROZ FRIEDBERG

Limitations on Disclosure

Attorney-Client Privilege

- Counsel
- Forensic Experts Hired by Counsel

Ohio Rev. Code § 2921.22(G)(1):

- Sections (A) and (D) do not require disclosure when information privileged between attorney and client (among a list of others)

SQUIRE SANDERS

STROZ FRIEDBERG

What to Expect from Law Enforcement

- Most police officers are not computer experts
  - Initial reports are often taken by a patrol officer
  - Follow-up investigations (if requested) may be conducted by investigator

- Do you need a Law Enforcement investigation?
  - Can you conduct an investigation in-house?
  - Can you hire outside experts to conduct an investigation?

SQUIRE SANDERS

STROZ FRIEDBERG

What to Expect from Law Enforcement

- Law enforcement will work to be minimally intrusive while collecting information needed
- The investigation will not be fast
  - Subject to prioritization of other cases
  - Subject to manpower and operational necessities
- You may not get all the information you need
  - Criminal evidence will likely not be released during the course of the investigation
  - Do not expect Law Enforcement to be a stopping point for civil discovery
  - Arrangements may be possible to allow disclosure of certain pieces of information

SQUIRE SANDERS

STROZ FRIEDBERG

HIPAA

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Pub. L. 104-191
  - Privacy Rule
    - Standards for Privacy of Individually Identifiable Health Information
    - Establishes standards protecting certain health information
  - Security Rule
    - Security Standards for the Protection of Electronic Protected Health Information
    - Establishes standards protecting certain health information in electronic form
  - Office for Civil Rights (OCR) enforces Privacy and Security Rules
- More at www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

SQUIRE SANDERS

STROZ FRIEDBERG

Stimulus Bill creates HITECH

- Signed by President Obama on 2/17/2009
- $19.2 billion for health IT
- HITECH Act (Title XIII of American Recovery and Reinvestment Act)
  - Most significant changes to HIPAA since promulgation of privacy and security standards
  - Most new HIPAA provisions effective 2/17/2010

SQUIRE SANDERS

STROZ FRIEDBERG

HITECH in a Nutshell

- Extends reach of HIPAA Privacy and Security Rules
- Applies directly to Business Associates
- Imposes breach notification requirements on Covered Entities and Business Associates
- Increases enforcement and penalties for privacy and security violations

SQUIRE SANDERS

STROZ FRIEDBERG

What is a Business Associate?

- Person or entity
  - Performing functions or activities
  - Involving the use or disclosure of protected health information
  - On behalf of, or provides services to, a covered entity
- A member of the covered entity's workforce is not a business associate
- September 23, 2013 deadline

SQUIRE SANDERS

STROZ FRIEDBERG

But I’m just a BA ...

SQUIRE SANDERS

STROZ FRIEDBERG

Examples of a Business Associate

- Third party administrator assisting health plan with claims processing
- CPA whose services involve access to PHI
- Attorney whose services involve access to PHI
- Consultant that performs utilization reviews for a hospital
- Health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer
- Independent medical transcriptionist providing services to a physician
- Pharmacy benefits manager for health plan's pharmacist network

SQUIRE SANDERS

STROZ FRIEDBERG

HITECH Act Implications for BAs

- Applies directly to BAs
- If breach of BA Agreement, BA must take reasonable steps: cure breach, terminate or report conduct to HHS
- BAs subject to HIPAA privacy and security requirements (including policies and procedures)
- BAs subject to criminal and civil penalties

SQUIRE SANDERS

STROZ FRIEDBERG

Thank You for Joining Our Webinar

Join Us for Part II of This Topic …

- My Data's Been Stolen: Now What? – Part II – November 21, 2013

Join Us for Our Next Call in This Series …

- The Anatomy of a Hospital-Physician Alignment Transaction – October 16, 2013

SQUIRE SANDERS

STROZ FRIEDBERG

Thank You for Joining Our Webinar

Questions?

SQUIRE SANDERS

STROZ FRIEDBERG

Thank You for Joining Our Webinar

Contact us with other topics, questions or issues:

- **Tom Zeno:** thomas.zeno@squiresanders.com
- **Emily Root:** emily.root@squiresanders.com
- **Scott Edelstein:** scott.edelstein@squiresanders.com

- **Tom Hibarger:** thibarger@strozfriedberg.com
- **Justin Root:** justin.root@ohioattorneygeneral.gov

SQUIRE SANDERS

STROZ FRIEDBERG

What Keeps You Up at Night?

Issues of Fraud and Abuse Compliance Series

39 Offices in 19 Countries