RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: LAW-W04

Managing Expectations: The SEC & FTC Target InfoSEC Compliance

MODERATOR:

Patrick Oot
Partner
Shook, Hardy & Bacon LLP
@patrickoot

PANELISTS:

David Shonka
Principal Deputy General Counsel
Federal Trade Commission

John Davis
Executive Director and Counsel
UBS AG

Jerami Kemnitz
Global Discovery Counsel
Wells Fargo

Randy Sabett
Special Counsel
Cooley LLP

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Please Participate:

www.pollev.com/RSA2015

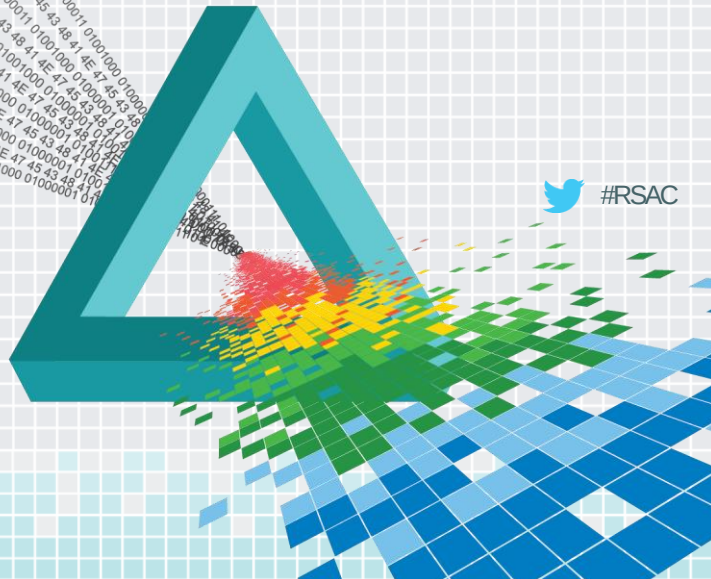
Overview

- Identify Recent Regulatory Initiatives at Executive Agencies
- Discuss Recent Information Security Indicatives at
- FTC, FCC and SEC
- Recent actions against organizations for failed information security
- Questions
- Consider how your organization might react to additional changes in regulation

RSAConference2015

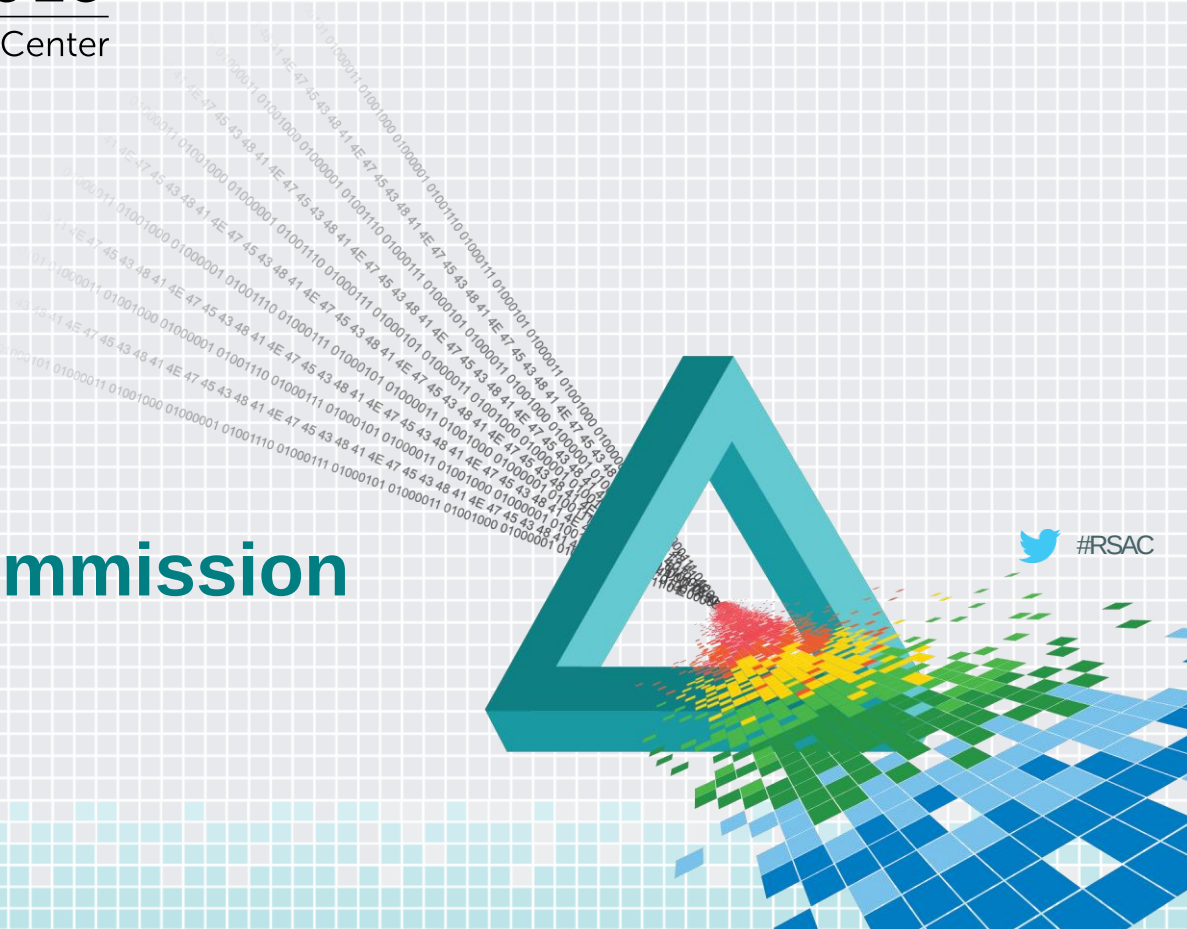
San Francisco | April 20-24 | Moscone Center

The statements and views of panelists are his or her own, and do not necessarily represent the views of their employer.



RSAConference2015

San Francisco | April 20-24 | Moscone Center



Federal Trade Commission (FTC)

Test Your Regulatory Skills

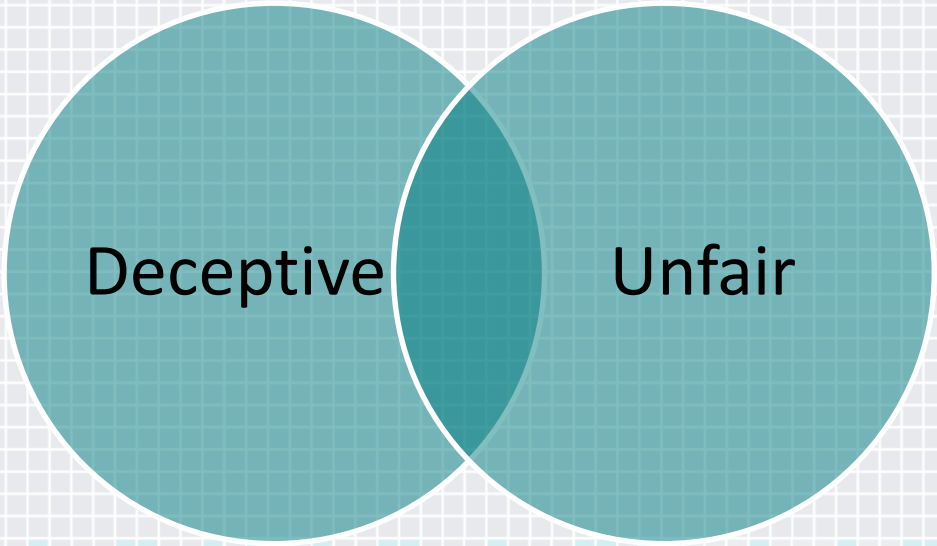
In Feb. 2015 Erica Entrepreneur a software developer launches Elephantine Enterprises, Inc. (EE) Her site links transaction information directly to users' e-mail address. EE employees can access transaction data with "PASSWORD" In March A precocious Edmund Elementary 3rd grader hacks and downloads her entire database. Were Erica's security measures reasonable?

1. Yes, she is a small start-up – should not be held to a high standard
2. Yes, She just launched and is within the sunrise period for compliance
3. No, Erica was unreasonable for using PASSWORD
4. No, but Erica is entitled to retaliate, even if her actions could wipe Edmund Elementary' s network

Federal Trade Commission Enforcement

Deception:

- Material Misrepresentation or Omission
- Express or Implied



Unfair

- Act or Practice Likely to Cause Substantial Harm to Consumers
- That Consumers cannot avoid
- And that has no countervailing benefit

Federal Trade Commission Enforcement

- FTC is the principal consumer protection and privacy agency. Responsible for law enforcement, public education and guides
- Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits **"unfair or deceptive acts or practices in or affecting commerce."**
- If a company makes **materially misleading statements or omissions** about privacy or data security that are likely to mislead reasonable consumers, such statements or omissions are deceptive.

Recent FTC Enforcement Actions

- *TRENDnet, Inc.*,
  - No. C-4426 (F.T.C. Jan. 16, 2014) (consent order).
- *FTC v. Wyndham Worldwide Corp. et al.*,
  - Civil No. 13-1887 (D.N.J. Apr. 7, 2014)
- *Craig Brittain*,
  - File No. 132-3120 (F.T.C. Jan. 29, 2015) (proposed consent)
- *FTC v. Sitesearch Corp. d/b/a LeapLab*
  - (D. Az. filed Dec. 23, 2014)

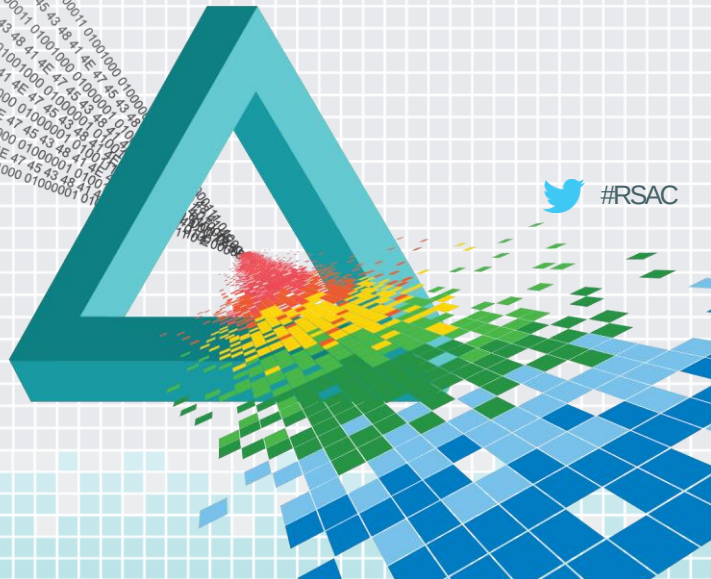
Federal Trade Commission (FTC) News

- FTC recently announced formation of its Office of Technology Research and Investigation (OTRI), an office meant to “ensure that consumers enjoy the benefits of technological progress without being placed at risk of deceptive and unfair practices.”
- The OTRI is the successor to the MTU, and will build upon their great work by tackling an even broader array of investigative research on technology issues involving all facets of the FTC’s consumer protection mission, including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data, and the Internet of Things.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Federal Communications Commission (FCC)



FCC Efforts re Cyber and Framework Adoption

- Advisory groups since 2001; Communications Security, Reliability and Interoperability Council (CSRIC)
- Multi-stakeholder with over 50 security experts appointed by FCC Chairman to develop and recommend practical cybersecurity best practices and solutions
- "The FCC was pleased to participate in [the NIST Framework dev't]. **Now the next phase of hard work begins. It is time to operationalize the framework within the communications sector to keep America's information economy strong**." – Tom Wheeler, FCC Chairman, February 2014
- Stakeholders must "create a new paradigm of cyber readiness" that must at once be **more dynamic** than traditional, slow-paced prescriptive regulation yet "demonstrably" more effective than "blindly trusting the market or voluntary best practices." – Chairman Wheeler, June 2014
- Report released March 19, 2015, with following recommendations:
  - adapting the voluntary Framework to effectively manage cybersecurity risk
  - sharing of cyber threat information among communications companies
  - using network availability as an indicator of successful cybersecurity risk management

FCC Privacy/Data Security Enforcement Efforts

- Three privacy-related actions in 2014, involving robocalls, violations of do-not-text requests, and unlawful marketing
- **$10M in October 2014** enforcement actions against two companies
  - Two carriers provided subsidized phone service to low income consumers and retained a third party vendor for various services, including data storage on dedicated servers
  - Data was stored in clear and accessible via the Internet using simple searches
  - FCC found violation of Sec. 222(a) (failure to protect customer proprietary information) and Sec. 201(b) (failure to notify was unjust or unreasonable practices)
- **$25M in April 8, 2015** enforcement action against AT&T
  - Call center employees in Mexico, Columbia, and Philippines found to be acquiring names and partial SSNs, then selling those to people who used them to unlock stolen AT&T phones that found their way to the secondary market
  - FCC again found violations of Sec. 222 and Sec. 201(b)
  - "As today s action demonstrates, the Commission will exercise its full authority against companies that fail to safeguard the personal information of their customers"

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Securities and Exchange Commission (SEC)

RSA Conference2015

San Francisco | April 20-24 | Moscone Center

“Cybersecurity threats know no boundaries. That’s why assessing the readiness of market participants and providing investors with information on how to better protect their online investment accounts from cyber threats has been and will continue to be an important focus of the SEC”

(SEC Chair Mary Joe White, Feb 3, 2015)

#RSAC

SEC Cybersecurity Examination Initiative

- The Office of Compliance Inspections and Examinations ("OCIE") protects investors through administering the SEC's nationwide examination and inspection program.
- On April 15, 2014, announced Cybersecurity Examination Initiative
- February 3, 2015 Cybersecurity Examination Exam Sweep Summary
- examined 57 registered broker-dealers and 49 registered investment advisers

Broader Governmental Initiative

- Financial Industry
  - Jan 2014: FINRA broker-dealer cyberexam sweep letters
  - May/Oct. 2014: NY State Department of Financial Services (DoFS) report and survey

  Each released reports in February/April 2015
- Overseas: regulatory inquiries and EC proposed directives on cybersecurity

OCIE Risk Alert:
Cyber Examinations focused on how firms:

- Identify cybersecurity risks
- Establish cybersecurity policies, procedures, and oversight processes
- Protect their networks and information
- Identify and address risks associated with remote access to client information, funds transfer requests, and third-party vendors
- Detect, and have experienced, unauthorized activity
- Report on incidents

Third Party Risk

- 2015 priority area of examination
  - DoFS considering regulations
- Industry reliance on providers for critical banking functions
- Perceived weak link
  - Traditional outsourcing co's (check payment; data processing, etc.)
  - Professional firms: e.g., accountants, law firms
    - Forthcoming Sedona Conference WG1 draft paper: *"Privacy and Information Security: Guidelines and Best Practices for Lawyers, Law Firms, and Other Legal Service Providers",* Shonka ed.; Davis contr.

Test Your Regulatory Skills

Green Mountain Financial is a publically traded exotic financial products broker. Prior to the earnings call Tom Technical used a readily accessible service account to access an encrypted finance server to obtain pre-announcement earnings information. Tom and his father made millions. GMF fired Tom and cooperated fully with SEC & DOJ. Is GMF in the clear?

A.) Probably, GMF cooperated. Only those that acted on the information can be charged under US Securities Law.

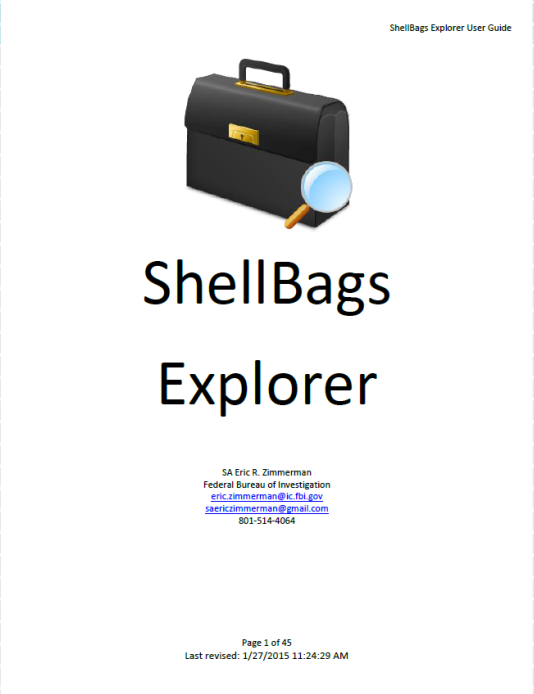
B.) Probably, GMF encrypted the drive – a reasonable precaution

C.) Maybe Not, financial regulations impose a duty on GMF to supervise and monitor employees

D.) Put Tom and his dad in the clink, regulations impose a duty on GMF to require employees to seek approval to trade in company stock

Securities and Exchange Commission Oversight

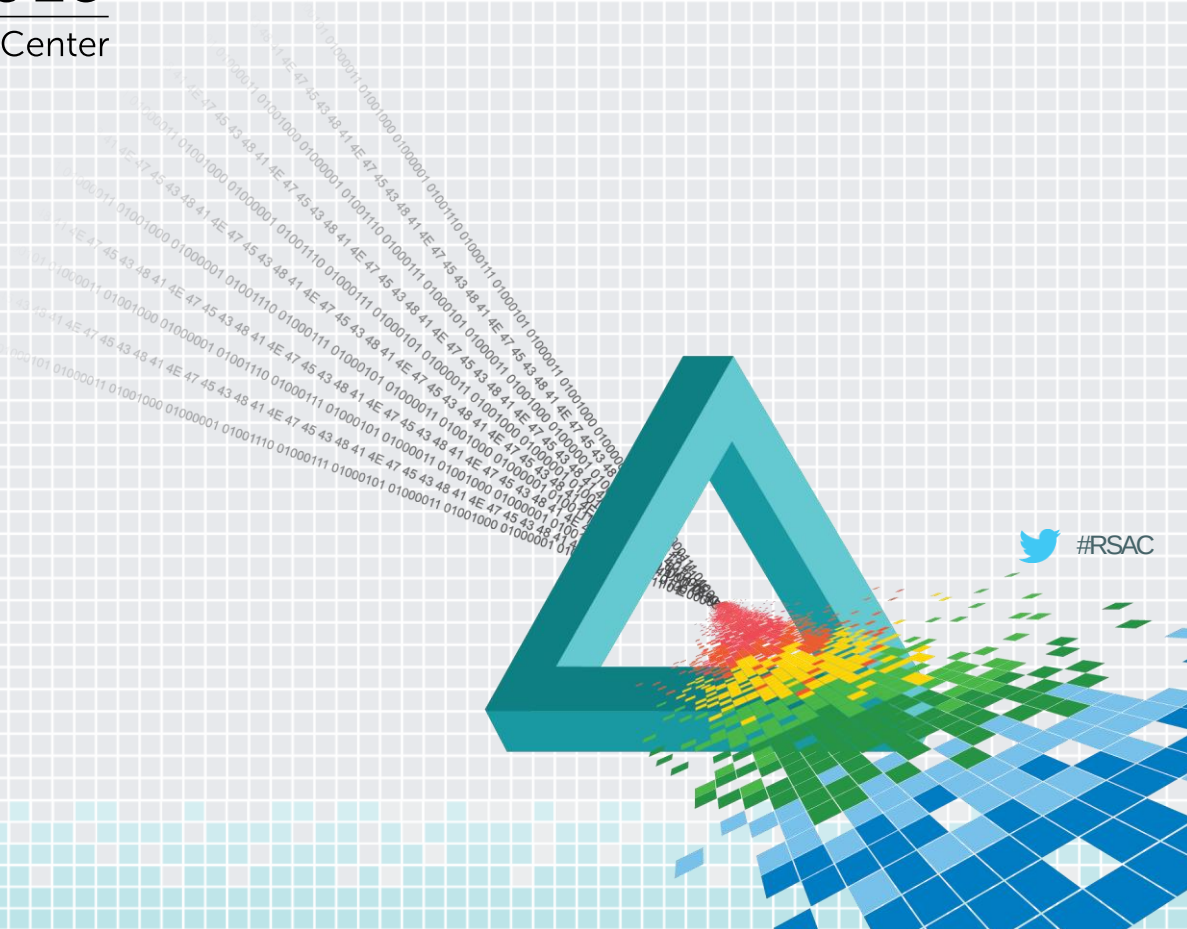
- Insider traders are usually charged with Section 17(a) of the Securities Act of 1933 and Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5
- However, risk of liability may exist for organization
- Exchange Act Section 15(g) requires that registered broker-dealers establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of their business, to prevent its misuse in violation of the securities laws by the broker-dealer or its associated persons.
- Misuse of Material Nonpublic Information (“MNPI”).



BUSTED!

Reference: SA Eric R. Zimmerman
Federal Bureau of Investigation

Questions?



Application

- Participate in the regulatory process
- Consider FTC and SEC Regulations, along with FCC enforcement actions, and how they might affect your business
- Consider reasonableness in information security practices
- Monitor dockets of active breach cases