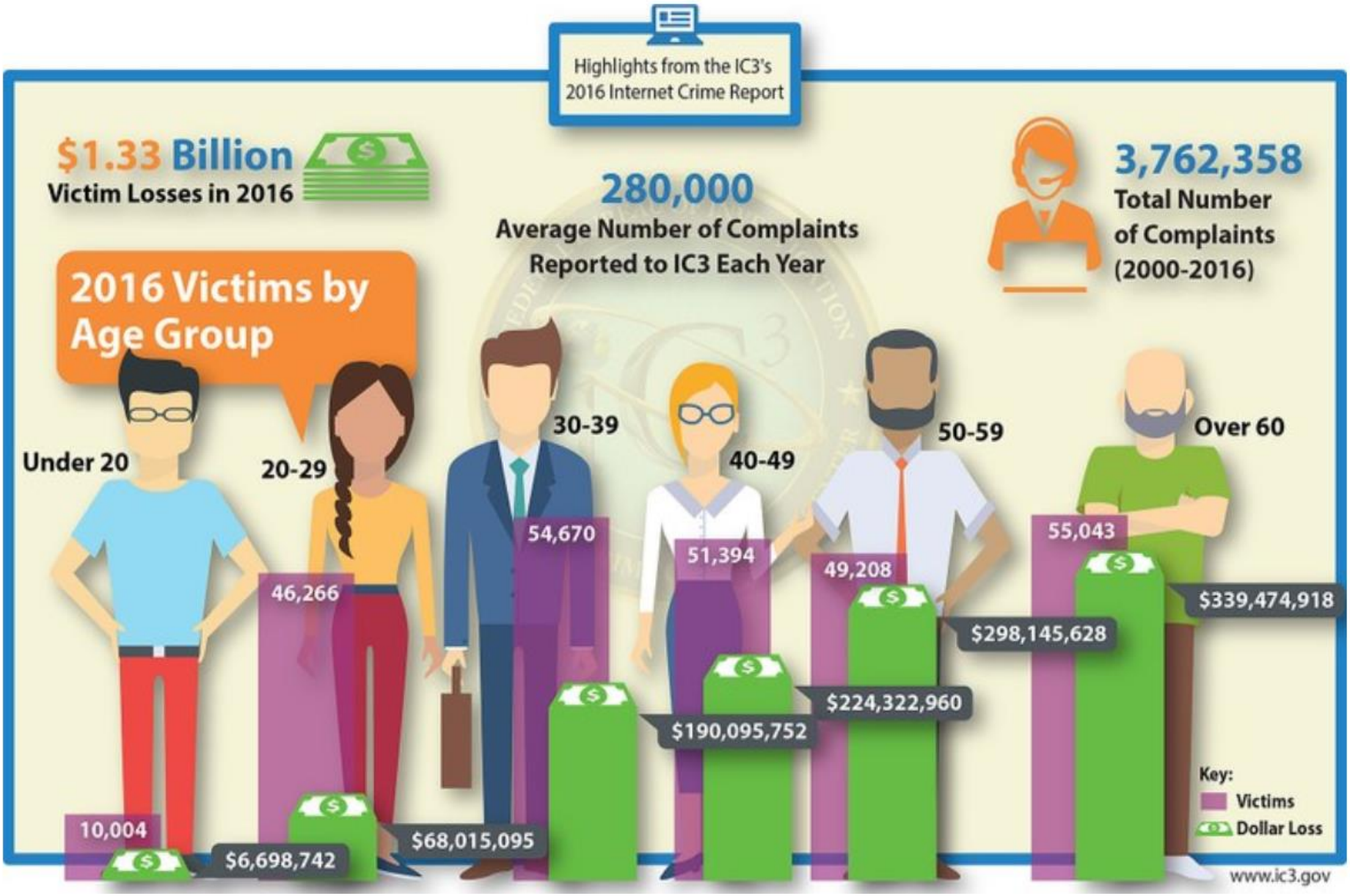
K&L GATES

2017 BOSTON INVESTMENT MANAGEMENT CONFERENCE

Social Media and Cybersecurity

Julia B. Jacobson, Partner, Boston
Michael W. McGrath, Partner, Boston
Richard F. Kerr, Partner, Boston

Proliferation of Cybersecurity Incidents


Highlights from the IC3's 2016 Internet Crime Report
$1.33 Billion
Victim Losses in 2016
280,000
Average Number of Complaints Reported to IC3 Each Year
3,762,358
Total Number of Complaints (2000-2016)
2016 Victims by Age Group
Under 20
20-29
30-39
40-49
50-59
Over 60
10,004
46,266
54,670
51,394
49,208
55,043
$6,698,742
$68,015,095
$190,095,752
$224,322,960
$298,145,628
$339,474,918
Key:
Victims
Dollar Loss
www.ic3.gov

WHY HACK?

1. Ransom – business pays hackers to resolve a problem
2. Competitive advantage – know what a competitor is doing and developing
3. Hacktivism – political gain
4. Nuisance – personal vendetta

SEC Guidance on Cybersecurity and Application of State Laws

CYBERSECURITY REGULATORY STANDARDS FOR INVESTMENT MANAGERS – THE BIG PICTURE

2014

- SEC Roundtable
- OCIE Risk Alert and Sweep Exams
- CFTC Best Practices

2015

- OCIE Risk Alert and Sweep Exam Summary
- FINRA Report on Cybersecurity Practices
- IM Guidance Update
- NFA Cybersecurity Rule
- Second OCIE Risk Alert
- Second Round of OCIE Sweep Exams
- SEC Enforcement

2016

- NFA Cybersecurity Self-Examination Questionnaire
- Morgan Stanley violation of Rule 30(a) of Regulation S-P

2017

- OCIE Risk Alert on Ransomware
- Second OCIE Risk Alert on Cybersecurity 2 Initiative

Future Initiatives

- More Interpretive Guidance?
- More Rulemaking?
- More Enforcement?
- NFA Examinations?

Primary Regulatory Authorities:

- Securities and Exchange Commission
- Financial Industry Regulatory Authority
- Commodity Futures Trading Commission
- National Futures Association
- Federal Trade Commission
- Federal and State Enforcement Authorities

Primary Legal Requirements:

- Regulation S-P (Safeguards Rule)
- Regulation S-ID (Identity Theft Red Flags)
- IAA Rule 206(4)-7 and ICA Rule 38a-1 (Compliance Rules)
- IAA Rule 204-2(g) and ICA Rule 31a-2(f) (Electronic Recordkeeping Rules)
- ICA Rule 30a-3 (Internal Controls)
- Disclosure Considerations
- Business continuity plans
- Suspicious activity reporting
- CFTC Regulations, Part 160.30
- FTC enforcement of Section 5 of FTCA
- State data breach and information security program requirements

RECENT SEC GUIDANCE

- 2017
  - OCIE Risk Alert: Observations from Cybersecurity Examinations (August 7, 2017)
  - OCIE Risk Alert: Cybersecurity Ransomware Alert (May 17, 2017)
- 2015
  - OCIE Risk Alert: OCIE's 2015 Cybersecurity Examination Initiative (September 15, 2015)
  - OCIE Risk Alert: Cybersecurity Examination Sweep Summary (February 3, 2015)

CYBERSECURITY REGULATORY LANDSCAPE IN 2018 AND BEYOND

- OCIE will continue to examine for cybersecurity compliance procedures, including testing the implementation of procedures and controls at firms
- Outstanding questions
  - The effect of state cybersecurity laws in the absence of SEC pre-emption
  - Enforcement actions in the absence of an actual breach
  - Impact of remedial measures on enforcement decisions
  - 20/20 hindsight: In the event of an actual breach, enforcement actions may be brought against firms with “reasonably designed” policies and “best practices”

Cybersecurity Readiness and Response

BE PREPARED

- ✓ Document cybersecurity roles and responsibilities
- ✓ Make cybersecurity a Senior Management/ Board issue
- ✓ Ensure cybersecurity policies are appropriate for risks – one size does not fit all
- ✓ Ensure cybersecurity policies address at least regular vulnerability assessments, malware detection and prevention, incident response plan and regulatory incident reporting requirements
- ✓ Train employees thoroughly and regularly
- ✓ Test incident response plan … and test again
- ✓ Conduct and document review of vendor cybersecurity practices prior to engagement and periodically throughout engagement

RESOURCES

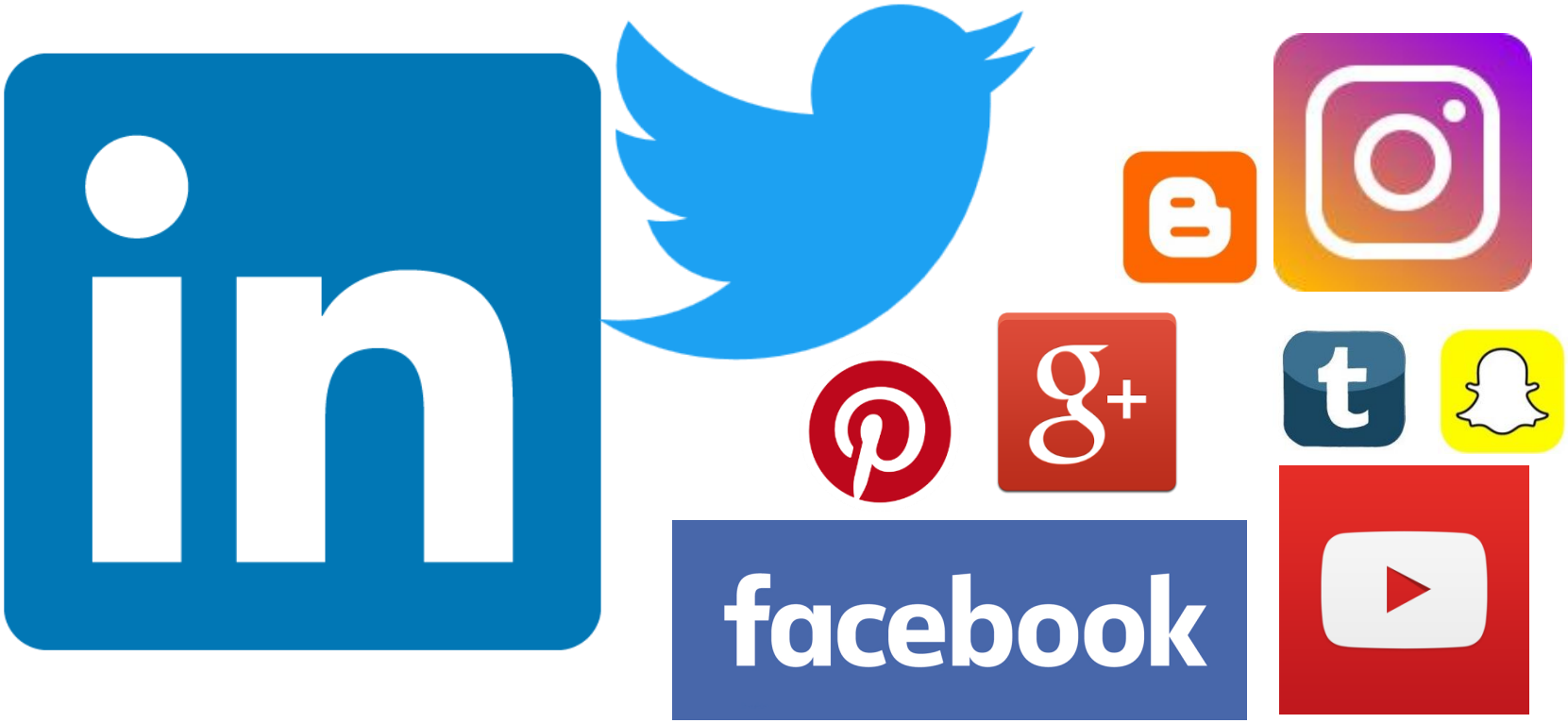
- National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*
- FFIEC Information Security Booklet
- (ISC)², Inc.
- *In re The Home Depot Inc.* Shareholder Derivative Litigation, case number 1:15-cv-2999, in the U.S. District Court for the Northern District of Georgia

Use of Social Media by Advisers and Brokers

WHAT IS SOCIAL MEDIA?

"Social Media is an umbrella term that encompasses various activities that integrate technology, social interaction and content creation. Social media may use many technologies, including, but not limited to, blogs, microblogs, wikis, photos and video sharing, podcasts, social networking and virtual worlds."

SEC National Exam Risk Alert (January 4, 2012)



APPLYING OLD STANDARDS TO NEW TECHNOLOGY

- Generally, there have been no new laws or regulations written to govern the use of social media
- Social media posts are considered to be:
  - Advertisements for purposes of investment adviser law and regulation subject to Section 206 of the Advisers Act and Rule 206(4)-1 thereunder, and
  - Communications with the public under the FINRA Rules subject to FINRA Rule 2210
- In addition to law and regulation governing content, social media posts present challenges for investment advisers and broker-dealers in complying with other regulations, including:
  - Compliance / supervision rules
  - Privacy regulation
  - Recordkeeping regulation

APPLICABLE SOCIAL MEDIA GUIDANCE

- SEC
  - OCIE National Examination Risk Alert, The Most Frequent Advertising Rule Compliance Issues Identified in OCIE Examinations of Investment Advisers (September 2017)
  - Form ADV Amendments, SEC Release No. IA-4509 (August 2016)
  - Division of Investment Management Guidance on the Testimonial Rule and Social Media (March 2014)
  - IM Guidance Update, Filing Requirements for Certain Electronic Communications (March 2013)
  - OCIE National Examination Risk Alert, Investment Adviser Use of Social Media (January 2012)

APPLICABLE SOCIAL MEDIA GUIDANCE

- FINRA
  - FINRA Regulatory Notice 17-18 (April 2017): Guidance on Social Networking Websites and Business Communications
  - Targeted Examination Letter (June 2013): Spot-Check of Social Media Communications
  - FINRA Regulatory Notice 11-39 (Aug. 2011) – Social Media Websites and the Use of Personal Devices for Business Communications
  - FINRA Regulatory Notice 10-06 (Jan. 2010) – Guidance on Blogs and Social Networking Websites
  - FINRA Regulatory Notice 07-59 (Dec. 2007) – Supervision of Electronic Communications

CELEBRITY ENDORSEMENTS

- November 1, 2017 - SEC issued a warning to celebrities and social influencers who use social media to encourage consumers to invest and/or purchase stocks
- Reminding Celebrity/Influencer must disclose the nature, source, and amount of compensation paid (directly or indirectly) in exchange for the endorsement

Similar to recent FTC actions under Guides Concerning the Use of Endorsements and Testimonials in Advertising.

COMMON PROBLEMS

- Third Party Posts – Investment adviser or broker-dealer may become liable for third party content under an adoption or entanglement theory
- “Likes” and “Shares” by third parties of content
- Real time nature of social media makes compliance review difficult
- Capturing content for recordkeeping purposes


Social Media and Cyber Risk

SOCIAL MEDIA AND CYBER RISK

Phishing Phase 1: Target Reconnaissance

- The phisher uses social media to conduct reconnaissance on a target and his or her profession and employer, friends and colleagues, patterns and habits, etc.
- The phisher learns as much about the target as possible so that the phisher can deceive the target into thinking that the phisher is someone that the target can trust

Phishing Phase 2: Baiting the Hook

- The phishing e-mail is sent by what appears as a trusted individual or legitimate source and often includes personal information that the Phisher obtained during the target reconnaissance
- The phishing e-mail directs the target to visit a fake and malicious website

ACTUAL PHISHING WEBSITE

SOCIAL MEDIA AND CYBER RISK: KEY TAKEAWAYS

- Inventory and monitor corporate social identities
- Make social media part of your incident response plan
- Train employees
- Develop policies. For example:
  - Password hygiene
  - Know how to report to social media platforms


Questions?