Agenda

CEFLI Compliance & Ethics Committee Meeting
Wednesday, January 23, 2019
2 PM EST/1 PM CST/12 Noon MST/11 AM PST
Dial In: (800) 239-9838
Passcode: 3646069

I. Welcome and Introduction. — Donald J. Walters

A. Antitrust Statement.

II. Approval of Minutes – December 12, 2018 Meeting. — The Committee

III. Issues for Review. — The Committee

A. Antifraud Practices and Monitoring Systems.

Fraudulent activities pose a constant challenge for life insurance company compliance and ethics professionals. To address these challenges, life insurance companies have implemented sophisticated antifraud detection practices and monitoring systems; including, special investigation units ("SIUs") that investigate suspected instances of fraudulent activity.

Many life insurance companies have implemented antifraud detection systems that allow companies to identify suspected instances of fraudulent activities perpetrated by agents, customers and other external parties.

Several Committee members have asked the Committee to discuss the types of fraud prevention measures companies may have in place to detect suspected fraudulent activities. Specifically, the following questions have been presented for discussion:

What is the most impactful external fraud prevention measure your company has implemented?
What types of reports and processes are utilized to monitor for possible agent fraud against your company as well as your customers?
What tools or online resources does your company use for fraud investigations? (Most importantly, what techniques may be used to investigate phone numbers, emails or addresses associated with fraudulent activity?)

The Committee will be asked to discuss company antifraud practices and monitoring systems designed to detect potential fraudulent activities by agents, customers and other external parties.

B. Financial Exploitation of the Elderly and Vulnerable Adults (New York Regulation 187).

As the elderly segment of our population continues to grow, life insurance companies and other financial services organizations have become increasingly aware of suspected instances of financial exploitation of the elderly and vulnerable adults and have developed appropriate strategies and teams to address these concerns.

Practices designed to prevent financial exploitation and abuse of the elderly and vulnerable adults may become more prominent across the industry in light of New York Regulation 187's requirement that an "insurer shall establish and maintain procedures designed to prevent financial exploitation and abuse.[1]"

This requirement raises a question regarding the types of reports and processes that may be utilized to monitor and prevent financial exploitation of the elderly and vulnerable adults.

The Committee will be asked to discuss their practices designed to monitor and prevent possible financial exploitation of the elderly and vulnerable adults and, specifically, what types of reports may be generated to demonstrate compliance with regulatory requirements designed to "prevent financial exploitation and abuse."

C. California Assembly Bill 2634 - Notification of Adverse Changes in the Current Scale of Non-Guaranteed Elements.

California Assembly Bill adds Section 10113.70 to the California Insurance Code which will require insurers to provide a summary notice to a policyholder of a flexible premium life insurance policy whenever the policy is subject to an adverse change in the current scale of nonguaranteed elements for a policy in effect on or after April 1, 2019. (See copy attached.)

The new law also requires an insurer to provide an in-force illustration of current and future benefits and values whenever the policy is subject to an adverse change in the current scale of nonguaranteed elements.

The notice requirements for an adverse change in the current scale of nonguaranteed elements for a policy goes into effect on or after July 1, 2019 and the requirement with respect to providing an in-in-force illustration is scheduled to take effect on or after July 1, 2020.

---

[1] ("Financial exploitation and abuse" is defined to mean improper use in an adult's funds, property or resources by another individual, including fraud, false pretenses, embezzlement, conspiracy, forgery, falsifying records, course property transfers or denial of access to assets.) 11 NYCRR 224.6(f)

A question has been presented concerning whether companies are interpreting the notification and illustration requirements as pertaining to ***each*** adverse change in the current scale of nonguaranteed elements (i.e., an increase in the cost of insurance) or whether the notification and illustration requirements pertain solely to a change company's current scale of nonguaranteed elements (i.e., a change in current cost of insurance tables).

The Committee will be asked to discuss whether they interpret the requirements of new California Insurance Code Section 10113.70 to provide a notification and illustration of an adverse change in the current scale of nonguaranteed elements as applying to each adverse change in the current scale of nonguaranteed elements (regardless of whether it may impact the policy owned by a consumer) or whether the notification and illustration requirement pertains solely to a change in the company's current scale of nonguaranteed elements (that relates specifically to the policy owned by a consumer).

D. Filing of Life Insurance Policy Illustration Certifications.

Section 11 D. (1) of the NAIC Life Illustration Model Regulation requires insurers to comply with the following:

> D. (1) The illustration actuary shall file a certification with the board and with the Commissioner:
>
> (a) Annually for all policy forms for which illustrations are used; and
> (b) Before a new policy form is illustrated.

For those companies that file illustrated life insurance policies with the Interstate Insurance Compact (the "Compact") and have been filing an annual illustration certification listing all policy forms for which illustrations are used, a question has been presented regarding whether a separate certification is also filed with the Compact before a new policy illustration is illustrated in those Compact states that have adopted the NAIC Life Illustration Model Regulation.

The Committee will be asked to discuss whether their company files both life insurance policy illustration certifications (i.e., an annual illustration certification listing all policy forms as well as a separate certification before a new policy is illustrated) through the Compact in those states that have adopted the NAIC Life Illustration Model Regulation.

E. OR Senate Bill 769 - Redacting of Social Security Numbers in Consumer Correspondence and Document Destruction Policies.

During 2018, the Committee discussed strategies associated with complying with the requirements of Oregon Senate Bill 769 which require the redacting of Social Security numbers in consumer correspondence and included requirements with respect to the treatment of Social Security numbers in document destruction practices. (See copy attached.

The Committee will be asked to discuss whether anyone has received any updates from the Oregon Insurance Administration regarding the impact of Oregon Senate Bill 769 on life insurer practices.

IV. Reporting Items. CEFLI Staff.

A. New State Insurance Commissioners.

The start of a new calendar year often marks the effective date of new legal and regulatory requirements. In the life insurance industry, the start of a new calendar year also marks the introduction of new state insurance commissioners in selected states due to prior year elections and/or new appointments.

In 2019, there will be 11 new state insurance commissioners. These changes are as follows:

State	New Commissioner	Former Commissioner
California	Ricardo Lara	Dave Jones
Connecticut	Paul Lombardo	Katherine Wade
Georgia	Jim Beck	Ralph Hudgens
Hawaii	Colin Hayashida	Gordon Ito
Kansas	Vicki Schmidt	Ken Selzer
Illinois	Karin Zosel	Jennifer Hammer
Michigan	Anita Fox	Patrick McPharlin
Minnesota	Steve Kelley	Fred Andersen (Acting)
New York	Linda Lacewell	Maria Vullo
Oklahoma	Glen Mulready	John Doak
Wisconsin	Tony Evers	Ted Nickel

B. NAIC Committee Assignments.

The NAIC recently announced its 2019 Committee Chairs and Vice Chairs.

Two Committee assignments of interest to CEFLI member companies include:

Life Insurance and Annuities (A) Committee

Chair: Doug Ommen, Commissioner, Iowa Insurance Division
Vice-Chair: Stephen C. Taylor, Commissioner, District of Columbia Department of Insurance, Securities and Banking

Market Regulation and Consumer Affairs (D) Committee

Chair: Chlora Lindley-Myers, Director, Missouri Department of Insurance, Financial Institutions and Professional Registration ("DIFP")
Vice-Chair: Allen W. Kerr, Commissioner, Arkansas Insurance Department

C. FINRA 2019 Risk Monitoring and Examination Priorities Letter.

FINRA recently released its 2019 Risk Monitoring and Examination Priorities Letter which identifies those subject matters that FINRA examination activities will focus on in the upcoming year. (See copy attached.)

The Letter is divided into distinct areas of concern including sales practice risks, operational risks, market risks and financial risks.

Subject areas noted as areas for in the Sales Practice Risks section of the Letter include:

- Suitability including Variable Annuities;
- Senior Investors;
- Anti-Money Laundering;
- Outside Business Activities and Private Securities Transactions; and
- Supervision.

D. SEC 2019 Examination Priorities.

The SEC's Office of Compliance Inspections and Examinations recently issued their 2019 examination priorities. (See copy attached.)

Areas for heightened focus during examinations in 2019 may include:

- Conflicts of Interest
- Senior Investors and Retirement Accounts and Products

- Cybersecurity
- Anti-Money-Laundering Programs

E. SEC Risk Alert - Advisor Texting and Social Media Use.

The SEC's Office of Compliance Inspections and Examinations recently issued a Risk Alert to outline observations from recent investment adviser examinations conducted by the SEC with a focus on electronic messaging. (See copy attached.) For purposes of this exam activity, "electronic messaging" included text/SMS messaging, instant messaging, personal email and personal or private messaging.

The Risk Alert offers examples of practices concerning the use of electronic messaging that the SEC believes may help advisers in meeting compliance obligations. The Risk Alert offers recommendations concerning policies and procedures, employee training and attestations, supervisory review and control over devices.

While the Risk Alert pertains solely to registered investment advisers, it may be helpful to inform those companies that may be considering strategies to permit use of texting/SMS messaging and other communication methods for their insurance producers.

F. FINRA Report on Selected Cybersecurity Practices.

Late last year, FINRA released its Report on Selected Cybersecurity Practices for broker-dealers firms. (See copy attached.)

The report outlines FINRA's observations regarding effective practices that firms have implemented to address certain cybersecurity risks.

Given the ongoing challenge that cybersecurity risks pose for the life insurance industry, it is hoped that this report may help life insurance companies in the assessment of their own cybersecurity practices.

G. Illinois Biometric Information Privacy Act Litigation – Rivera/Weiss v. Google

The US District Court for the Northern District of Illinois (Eastern Division) recently issued an opinion in favor of Google and dismissed plaintiffs' claims that Google's practice of automatically creating a faced template when android users upload photos taken on their smart phone to Google's cloud-based service violates the Illinois Biometric Information Privacy Act. (See copy attached.)

Illinois was the first state in the country to regulate the collection of biometric information, which includes facial recognition data. Biometric information is being explored by life insurers as a means to make the life insurance underwriting process more efficient.

This may be an important case as social media companies (and life insurance companies) increasingly explore the use of biometric information for targeted advertising and filtered content.

H. Wells Fargo Agrees to Pay $575 Million Regarding Sales Practices.

Wells Fargo recently announced that it has agreed to pay $575 million to resolve claims from 50 state attorneys general and the District of Columbia related to opening millions of fake accounts for consumers in several states.

This settlement between the bank and state attorneys general is separate from actions taken by federal regulators.

Wells Fargo serves as a continuing reminder of the importance (and cost) of establishing a sound culture of compliance and ethics within financial services organizations.

V. CEFLI Activities.

A. Mark Your Calendar - CEFLI Webinar - Cost of Insurance - Tuesday, January 29.

CEFLI will be conducting a webinar with representatives from CEFLI's Affiliate Member law firm, Drinker Biddle, on the Cost of Insurance Litigation and Regulatory Developments on Tuesday, January 29 at 1 PM EST/12 Noon CST/11 AM MST/10 AM PST.

Please mark your calendar and plan to join us!

B. Open Invitation - Faculty Members for CEFLI Webinars.

As we embark on a new year, CEFLI would like to invite members of the Committee to consider possibly serving as faculty members for future CEFLI webinars.

Please bear in mind that CEFLI webinars also serve as an excellent professional development opportunity for members of your staff that may not have regular access to public speaking venues.

Please contact Kelly Ireland on CEFLI's staff if you may (or a member of your staff) have an interest in serving as a faculty member at an upcoming CEFLI webinar.

VI. Next Meeting.

The next meeting of the Committee is scheduled to take place:

February 13, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST

The Committee will hold its remaining 2018 meetings as follows:

March 20, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
April 17, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
May 15, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
June 11, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
July 24, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
August 14, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
September 25, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
October 16, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
November 13, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
December 18, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST

Please mark your calendar and plan to join us!

VII. Other Business.

The Committee will be asked to identify and discuss any other business to be brought before the Committee.

DRAFT

Minutes
Meeting of the
CEFLI Compliance & Ethics Committee
December 12, 2018
2 PM EDT/1 PM CDT/11 AM PDT

A meeting of the CEFLI Compliance & Ethics Committee (the "Committee") was held via conference call on Wednesday, December 12, 2018 at 2 PM EDT/1 PM CDT/11 AM PDT.

The following CEFLI member company representatives participated in the meeting:

Molly Akin (Ohio National)
Dwain Akins (American National)
Marcie Allen (Texas Life)
Shannon Aussieker (Country Financial)
Jenna Austin (Guggenheim)
Erich Axmacher (Securian)
Brendan Bakala (Catholic Order of Foresters)
Chad Batterson (Athene USA)
Nicole Blakney (State Farm)
Kate Blalock (Western & Southern)
Vickie Bulger (Primerica)
Laura Bullard (Foresters)
Susan Burke (SunLife)
Dana Cook (Assurity)
Steve Corbly (Cincinnati Lifel)
Allison Corrado (Lombard International)
Jacquie Crader (Cuna Mutual)
John Cunningham (Fidelity Investments)
\Bill Dauksewicz (Protective)
Kathy Deputy (State Farm)
William Dunker (Principal)
Jessica English (Thrivent)
Bruce Eschbach (Texas Life)
Chad Eslinger (Voya)
Rita Fenani (Pacific Life)
Csaba Gabor (Global Atlantic Financial Group)
Patrick Garcy (Sagicor)

Paula Gentry (Cincinnati Financial)
Angela Gilsinn (Sun Life)
Jim Golembiewski (Sagicor)
Meagan Gonzalez (Oxford Life)
David Griffin (Baltimore Life)
Teresa Harvey (F&G Life)
Traci Hawkins (Trustmark)
Dennis Herchel (SBLI)
Amariliz Johnson (Jackson National)
Marty Karp (Oxford Life)
Lorna Katz (CNO Financial)
Keith Kirkley (Protective)
Matt Klein (Principal)
Jennifer Knabe (Ohio National)
Samantha Knackmuhs (State Farm)
Michele Kulish Danielson (American Enterprise)
Daniel Leblanc (SBLI)
Laurie Lewis (Amica)
Kevin Mechtley (Sammons Financial Group)
Rhonda Monroe (Jackson National)
Karoll Moran (Amica)
Sabrina Olender (Foresters)
Liza Perry (USAA)
Meghan Phillips (Principal)
Michelle Ross (Lombard International)
Sally Roudebush (Lincoln Heritage)
Heather Russo (Illinois Mutual)
Scott Schabel (Jackson)
Michael Schwalllie (Ohio National)
Ryan Schwoebel (Protective)
Sabrina Siddeeq (CNO Financial)
Stephen Smith (Protective)
Jeff Stafford (CNO Financial)
Carmella Storto (Oxford Life)
Lori Straight (Sammons)
Carla Strauch (Thrivent)
Kristen Thomas (Jackson National)
Betsy Treiber (Securian)
Bill Turner (American Fidelity)
Alan Walton (Symetra)
Jaime Waters (EquiTrust)
Larry Welch (Citizens, Inc.)
Lynee Welding (Midland National)
Stacey White (American National)
Emily Wilburn (Illinois Mutual)

Kelly Ireland and Donald J. Walters of CEFLI also participated in the meeting.

I. Welcome and Introduction.

The meeting began with a recitation of CEFLI's anti-trust statement.

II. Approval of Minutes – November 14, 2018 Meeting.

On motion, duly made and seconded and unanimously carried, the Committee: RESOLVED, that, the Minutes of the November 14, 2018 meeting are hereby approved.

III. Issues for Review.

A. Role of Compliance in Anti-Money-Laundering.

The Committee was asked to discuss their company practices with respect to AML legal and regulatory requirements and the role compliance plays in achieving your company's AML compliance objectives.

A Committee Member offered that their company had appointed a Chief AML Officer that resided in Compliance with designated AML contacts housed in various business units. There is no standalone AML department. A Chief AML officer has also been appointed for their subsidiary. For certain SARs decisions an AML Working Group will be convened.

Other Committee Members reported having a similar structure in place with a parent company Chief AML Officer and business line AML officers all of whom report up to the Chief Compliance Officer who is also involved from a testing and monitoring perspective.

B. Filing of Suspicious Activity Reports ("SARs").

The Committee was asked to discuss their practices with respect to the filing of SARs, including:

- Whether the volume of filing of SARs has changed over the past year;
- Whether the company utilizes the checkbox to denote suspected instances of suspicious activity that may be related to a senior, and;
- Whether there are additional steps the company takes with respect to filing a SAR (e.g., referral to internal audit, SIU, etc.).

A Committee Member indicated that this had not been a typical year for SAR filing and that their experience tends to vary widely from year to year. They do

utilize the check box to indicate possible activity involving seniors and, when filing any SAR, the SIU Director must approve the filing.

Another Committee Member reported that, while Compliance handles the filing of SARs, they may bring a SAR filing to the attention of other departments in an effort to improve processes such as sales or customer service practices.

C. Annuity Surrender Requirements - CA AB 1398 (CA Ins. Code § 10168.45).

Earlier this year, California enacted into law Assembly Bill 1398 pertaining to annuity surrender benefits added a new Section 10168.45 to the California Insurance Code. The law applies to non-variable, deferred annuity contracts issued on or after January 1, 2019 for which payments have not commenced.

Among its pertinent provisions, the law contains requirements with respect to:

- Limiting the information an insurer may require on a surrender form; and
- Allowing insurers to request a signature guarantee only if there is reason to believe a fraudulent situation may occur.

The Committee was asked to discuss their compliance strategies to address the requirements of California Insurance Code Section 10168.45 and whether these strategies will be applied exclusively to California-related business or whether they may be implemented on a nationwide basis.

A Committee Member indicated that they did not intend to treat California requests differently than other surrender requests. Their practice is to compare the signature on the surrender form to that on file for the contract.

This was echoed by other Committee Members, though one company added that when there are concerns about fraud, they may ask for a notarized surrender request.

D. Redacting of Social Security Numbers in Consumer Correspondence and Document Destruction Policies – OR Senate Bill 769.

The Committee discussed previously a new Oregon law that pertains to the use of Social Security numbers in consumer correspondence. The new law prohibits the printing of a consumer's SSN on mail to the consumer that s/he did not request and requires the SSN to be redacted on documents the consumer did request.

The Committee was asked to discuss their company's strategies to comply with the requirements of Oregon Senate Bill 769 pertaining to the use of SSNs on correspondence to consumers.

A Committee Member indicated that, after experimenting with various ways to "redact" the SSN, they have decided to place stickers over any SSN that is printed on documents being mailed to consumers in Oregon. While their systems will "X" out the first 5 digits, they feel it will be administratively easier to use stickers to cover any SSN being mailed out in Oregon rather than remove/redact depending on whether the consumer requested the document or not.

A Committee Member mentioned that the ACLI was intending to engage Oregon to discuss this issue and Mr. Walters offered to follow-up with the ACLI and report back to the Committee.

E. Central Clearinghouse for Vendor Compliance with New York's Cybersecurity Regulation.

New York's Cybersecurity Regulation (23 NYCRR 500) includes requirements for "covered entities" such as insurance companies to conduct a risk assessment of the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

As part of this risk assessment, life insurance companies are required to develop appropriate policies and procedures for due diligence and/or contractual protections related to third-party service providers.

Recent discussions have indicated a possible interest in establishing a standardized form to collect information from various third-party service providers for life insurance companies.

The Committee was asked to discuss whether there may be interest in establishing a standardized form to obtain information from third-party service providers and, if so, whether establishing a consortium or "Clearinghouse" (such as CEFLI's Annuity Suitability Clearinghouse) to gather this type of information may represent an efficient way for life insurers to comply with the third-party service provider requirements of New York's Cybersecurity Regulation.

A Committee Member reported that they have been working with a vendor (Prevalent) to develop and send a 174-question survey to selected parties (75 to date). They plan to review the collected information for completeness before determining next steps.

Another Committee Member suggested that the search for an efficient solution is being driven by the interpretation that third party distributors are considered third party vendors for the purpose of the NYDFS Cybersecurity Regulation, which raises the issue of one TPD who sells for many insurers having to undergo

multiple assessments (similar to concerns that arose from the Suitability Model's third-party certificate of compliance requirement).

It was reported that LICONY and LIMRA have hosted calls about this and are considering possible solutions such as developing a standardized questionnaire and duplicating the LIMRA approach to satisfying AML training requirements.

A Member Company indicated that the CEFLI Suitability Clearinghouse could be a potential model for the due diligence process pertaining to this issue.

Member Companies were encouraged to consider how CEFLI might help with reducing risk and meeting the compliance requirements of the NYDFS Reg and let CEFLI staff know that there is interest in this.

F. Denial of Approval of Wellness or Preventative Care Benefits – Michigan DIFS.

It has recently come to our attention that the Michigan Department of Insurance and Financial Services ("DIFS") has begun indicating that it will not approve wellness and/or preventative care benefits offered in association with fixed indemnity products such as critical illness or hospital indemnity coverage. Further, the DIFS has suggested to a member company that products DIFS approved just a few months ago (which remain approved) are not permitted, but DIFS has made no attempt to formally re-open/disapprove the filings it previously approved a few months ago.

The Committee was asked whether they are aware of a change in position on wellness/preventative care benefits in association with indemnity products by the DIFS or whether they may have any experience with such "informal" disapprovals of previously-approved products by the Michigan DIFS.

The Committee Member who raised this issue for discussion wanted others to be aware of this and indicated that their concern has to do with the informal way the DIFS is going about this; trying to say an approved filing is no longer approved without any formal process for re-review.

G. New York Regulation 187 - Training Requirements.

New York Regulation 187 contains requirements for insurers to ensure that every producer recommending any transaction is adequately trained.

Section 224.6(e) of the Regulation reads in pertinent part:

> *"An insurer shall be responsible for ensuring that every producer recommending any transaction with respect to the insurer's policies is adequately trained to make the*

> *recommendation in accordance with the provisions of this Part, but an insurer shall not be required to warrant that a producer is acting in the consumer's best interest." (Underscore added.)*

Some have read this provision to require insurers to train producers on the overall requirements of the Regulation and not solely on the insurer's products.

The Committee was asked to discuss their interpretation of Section 224.6 (E) of New York Regulation 187 and their plans to develop training policies and procedures to address this requirement.

A Committee Member indicated that they were interpreting the NY Reg broadly, but felt that informing producers of the training requirement with a summary and link to the Regulation was sufficient to meet the requirement. The company also requires annual certification by producers and registered representatives as to their understanding of the requirement.

Another Committee Member reported taking a similar approach and they are also planning to add information pertaining to this requirement to their product-specific training offered in conjunction with satisfying the Suitability Model training requirements (have added Reg 60 information and will also add Reg 187 information to this training as well).

IV. Reporting Items.

A. NAIC Fall National Meeting.

CEFLI staff reported that the NAIC conducted its Fall National Meeting in San Francisco on November 15-18.

The NAIC Annuity Suitability (A) Working Group continued to explore revisions to the NAIC Suitability in Annuity Transactions Model Regulation. The Working Group will continue efforts to develop a "Model Draft" which could be shared with the SEC to inform its analysis of the proposed Regulation Best Interest.

In addition, the NAIC Big Data (EX) Working Group of the Innovation and Technology (TX) Task Force is shifting its focus toward the life insurance industry in exploring techniques that companies apply to verify the accuracy of data used in accelerated and non-traditional life insurance underwriting.

B. CEFLI Advisory Committee.

CEFLI staff reported that CEFLI's Advisory Committee met on November 28 to explore a broad range of issues. The Advisory Committee is comprised of representatives from the SEC, FINRA, NAIC, and NAIFA, among others, who

discuss potential compliance challenges “on the horizon” for the life insurance industry.

Among issues discussed by the Committee included: the SEC’s Rule Proposals including Regulation Best Interest, revisions to the NAIC Suitability in Annuity Transactions Model Regulation, final amendments to New York Regulation 187, state proposed fiduciary rules, and use of various data sources in accelerated underwriting of life insurance products.

C. Reminder: December 17 Deadline - NYDFS Section 308 Letter - Underwriting Guidelines and Practices.

CEFLI Staff reported that the New York Department of Financial Services recently issued a Section 308 Letter requesting insurers to provide underwriting guidelines and practices related to criminal history or civil dispute history.

The response to the Section 308 letter is due on or before December 17, 2018.

D. FINRA Releases 2018 Examination Findings Report.

CEFLI Staff reported that FINRA recently released its 2018 Examination Findings Report. This is the second year in which FINRA has developed such a report as an outgrowth of the FINRA 360 initiative.

The Report highlights concerns regarding suitability for retail customers and, specifically, unsuitable variable annuity recommendations. Other areas of concern included inadequate supervisory systems and lack of documentation of investigations of potentially suspicious activities.

E. SEC Whistleblower Office Sees 18% Increase in Tips in 2018.

CEFLI Staff reported that the SEC Whistleblower Office recently issued its 2018 Annual Report to Congress which noted that the SEC received 5,282 whistleblower tips in 2018 which represented and 18% increase on a year-to-year basis.

F. Congressional Leadership Changes.

1. Senator Charles Grassley (R-IA) will be the next Chair of the Senate Finance Committee due to the retirement of current Chair, Senator Orin Hatch (R-UT).
2. Representative Maxine Waters (D-CA) is anticipated to become the new Chair of the House Financial Services Committee. According to reports, she has instructed her staff to begin developing a new subcommittee tentatively re-named the Investor Protection,

Entrepreneurship and Capital Markets Subcommittee which will focus on annuities and fiduciary issues.

G. NAIC Officer Elections.

CEFLI Staff reported that the following officers were elected at the NAIC Fall National Meeting:

- **President:** Maine Insurance Superintendent Eric A. Cioppa
- **President-Elect:** South Carolina Insurance Director Raymond G. Farmer
- **Vice President:** Hawaii Insurance Commissioner Gordon I. Ito
- **Secretary-Treasurer:** Idaho Insurance Director Dean L. Cameron

V. CEFLI Activities.

A. Mark Your Calendar - CEFLI Webinar - 2018 Year in Review - Tuesday, December 18.

CEFLI will be conducting a 2018 Year in Review webinar on Tuesday, December 18 at 1 PM EST/12 Noon CST/11 AM MST/10 AM PST.

Please mark your calendar and plan to join us!

B. Regulation 187 Issue Forum - Wednesday, December 19 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST.

CEFLI will be conducting the next meeting of its Regulation 187 Issue Forum next Wednesday, December 19 at 2 PM EST/1 PM CST/12 Noon MST/11 AM PST.

C. Annuity Suitability Benchmarking Study.

CEFLI will be issuing its Annuity Suitability Benchmarking Study within the next several days. The Annuity Suitability Benchmarking Study will be available for all CEFLI member companies via CEFLI's website.

VI. Next Meeting.

The Committee will hold its next meeting on January 23, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST

The Committee will hold further 2019 meetings as follows:

February 13, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST

March 20, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
April 17, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
May 15, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
June 11, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
July 24, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
August 14, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
September 25, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
October 16, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
November 13, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST
December 18, 2019 - 2 PM EST/1 PM CST/12 Noon MST/11 AM PST

Please mark your calendar and plan to join us!

VII. Other Business.

There being no further business to discuss, the meeting was adjourned.

Assembly Bill No. 2634

CHAPTER 545

An act to add Section 10113.70 to the Insurance Code, relating to insurance.

[Approved by Governor September 19, 2018. Filed with Secretary of State September 19, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2634, Chau. Life insurance.

Existing law requires an insurer transacting life insurance in California to register its policies with the Insurance Commissioner and comply with specified provisions of the Insurance Code relating to, among others, reserve liabilities, capital requirements, and disclosure requirements for replacement of life insurance policies. Existing law regulates illustrations used in the sale of a life insurance policy. Existing law requires an insurer to provide notice to the policyholder of a life insurance policy upon an increase of premium if that policy provides for premium changes, as specified.

For a policy in effect on or after April 1, 2019, this bill would require an insurer to provide a summary notice to a policyholder of a flexible premium life insurance policy whenever the policy is subject to an adverse change in the current scale of nonguaranteed elements, as defined. The bill would require the summary notice to include specified information and language about the adverse change. The bill would also require an insurer, for a flexible premium life insurance policy for which illustrations are used in effect on or after April 1, 2019, to provide an inforce illustration of current and future benefits and values whenever the policy is subject to an adverse change in the current scale of nonguaranteed elements. The bill would impose the notice requirements to an adverse change that is scheduled to take effect on or after July 1, 2019, and would impose the illustration requirement to an adverse change that is scheduled to take effect on or after July 1, 2020.

The people of the State of California do enact as follows:

SECTION 1. Section 10113.70 is added to the Insurance Code, to read:

10113.70. (a) (1) Whenever a flexible premium life insurance policy is subject to an adverse change in the current scale of nonguaranteed elements, as soon as practicable, but no later than 90 days before the effective date of the adverse change in the current scale of nonguaranteed elements, the insurer shall provide a summary notice and, if the policy is designated as one for which illustrations shall be used, an inforce illustration of current

and future benefits and values. The illustration or illustrations shall be based on the insurer's illustrated scale after the effective date of the adverse change in the current scale of nonguaranteed elements.

(2) An inforce illustration provided pursuant to this section shall comply with the requirements of subdivisions (a) and (b) of Section 10509.955 and subdivisions (a) and (e) of Section 10509.956.

(b) The summary notice shall be in no less than 12-point type, and the illustration and summary notice shall contain the following language in boldface type: "IMPORTANT: NOTICE OF CHANGE IN NONGUARANTEED ELEMENTS OF YOUR POLICY."

(c) The summary notice shall include the information required by paragraphs (1) to (5), inclusive, and the language set forth in paragraphs (6) to (8), inclusive:

(1) The name of each nonguaranteed element in the current scale of nonguaranteed elements that is subject to an adverse change.

(2) The definition of each nonguaranteed element in the current scale of nonguaranteed elements that is subject to an adverse change.

(3) A statement identifying the current rate or charge for each nonguaranteed element and the new rate or charge for each nonguaranteed element, with reference to the current scale of nonguaranteed elements, including the percentage change in the nonguaranteed element that the adverse change represents.

(4) An explanation that the adverse change in the current scale of nonguaranteed elements is based on expectations of the future cost of providing the benefits under the policy, and that the adverse change to the current scale of nonguaranteed elements will reduce the accumulation value and may increase the risk of policy lapse based on continued payment of current premiums.

(5) The date the adverse change to the current scale of nonguaranteed elements will take effect.

(6) "Policy information:

Last policy anniversary date: ____

Next policy anniversary date: ____

Current accumulation value: ____

Current cash surrender value (accumulation value minus any surrender charges and policy loans): ____"

(7) "Your options:

Take no action: This option will reduce the accumulation of your policy. Additional premiums will be required at some point in order to maintain your coverage if not otherwise adequately funded to maintain coverage.

Pay additional premiums: You may choose to pay additional premiums starting now to maintain your policy's accumulation value and death benefit coverage for the level and period anticipated before the increase.

Reduce the face value of your policy: If your policy is not already at the minimum value specified on your policy, you may choose to reduce the specified amount on your policy to a level that will be supported by the

amount and years of the premium payments you would like to pay. Please note that reducing the specified amount may result in a surrender charge.

Surrender your policy: You may choose to surrender your policy for the current cash surrender value. Before you decide to surrender your policy, you should consult your tax, insurance, or financial advisor.

Convert your policy (applicable only if your policy includes a conversion or exchange privilege in the contract): If you wish to maintain life insurance coverage but are unable to pay increased premiums to keep your policy in force, you may choose to convert your flexible premium life insurance policy to a different type of life insurance policy we offer, subject to the terms of conversions listed in your policy, which may better suit your financial needs."

(8) "We understand that you may have further questions about this change or the options available to you. You may call your agent or our customer service team at [insert customer service toll-free telephone number and hours of operation]."

(d) As used in this section:

(1) "Adverse change" means a change to the current scale of nonguaranteed elements that increases or may increase a charge, or reduces or may reduce a benefit to the policy owner, other than a change in a credited interest rate or an index account parameter based entirely on changes in the insurer's expected investment income or hedging costs.

(2) "Current scale of nonguaranteed elements" means the nonguaranteed elements, as defined in subdivision (m) of Section 10509.953, that apply to a policy in the current year and in future years, unless changed by the insurer.

(3) "Index account parameter" means a feature impacting the net credited rate for an index account, such as participation rate, cap, or spread.

(e) This section does not prohibit an insurer from including additional information in the notice that is specific to the policy for which the notice is sent, so long as it meets the requirements of this section.

(f) This section does not apply to a corporate-owned life insurance policy permitted by Section 10110.4 under which all benefits are payable to the corporate policy owner.

(g) (1) This section shall apply to a flexible premium life insurance policy in effect on or after April 1, 2019.

(2) Notwithstanding paragraph (1), the notice requirement of this section shall apply to an adverse change in the current scale of nonguaranteed elements that is scheduled to take effect on or after July 1, 2019.

(3) Notwithstanding paragraph (1), the illustration requirement of this section shall apply to an adverse change in the current scale of nonguaranteed elements that is scheduled to take effect on or after July 1, 2020.

O

2017 ORS 646A.620[1]

Prohibition on printing, displaying or posting Social Security numbers

• exemptions

(1) Except as otherwise specifically provided by law, a person may not:

(a) Print a consumer's Social Security number on mail to the consumer that is:

(A) Material the consumer did not request; **or**

(B) Part of any documentation the consumer requested for a transaction or service, unless the Social Security number is redacted.

(b) Print a consumer's Social Security number on any card required for the consumer to access products or services provided by the person.

(c) Publicly post or publicly display a consumer's Social Security number unless the Social Security number is redacted. As used in this paragraph, "publicly post or publicly display" means to communicate or otherwise make available to the public.

(d) Dispose of, or transfer to another person for disposal, material or media that display a consumer's Social Security number unless the person makes the Social Security number unreadable or unrecoverable or ensures that any person that ultimately disposes of the material or media makes the Social Security number unreadable or unrecoverable.

(2) This section does not prevent the collection, use or release of a Social Security number as required by state or federal law or rule adopted by the Chief Justice of the Supreme Court, the Chief Judge of the Court of Appeals or the judge of the Oregon Tax Court and does not prevent the use or printing of a Social Security number for internal verification or administrative purposes or to enforce a judgment or court order.

(3) This section does not apply to records that must be made available to the public under state or federal law or rule adopted by the Chief Justice of the Supreme

Court, the Chief Judge of the Court of Appeals or the judge of the Oregon Tax Court.

(4) This section does not apply to a Social Security number in any of the following records or copies of records in any form or storage medium maintained or otherwise possessed by a court, the State Court Administrator or the Secretary of State:

(a) A record received on or before October 1, 2007;

(b) A record received after October 1, 2007, if, by state or federal statute or rule, the person that submitted the record could have caused the record to be filed or maintained in a manner that protected the Social Security number from public disclosure; **or**

(c) A record, regardless of the date created or received, that is:

(A) An accusatory instrument charging a violation or crime;

(B) A record of oral proceedings in a court;

(C) An exhibit offered as evidence in a proceeding; **or**

(D) A judgment or court order. [2007 c.759 §11; 2017 c.254 §1]

---

[1] Legislative Counsel Committee, *CHAPTER 646A—Trade Regulation*, https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html (2017) (last accessed Mar. 30, 2018).

2019 Risk Monitoring and Examination Priorities Letter

January 2019

Topics

Introduction

The 2019 Risk Monitoring and Examination Priorities Letter identifies topics that FINRA will focus on in the coming year. The letter begins with materially new priorities and then discusses priorities in areas of ongoing concern, but with an emphasis on aspects of those topics we have not articulated in prior letters. Unlike previous Priorities Letters, we do not repeat topics that have been mainstays of FINRA's attention over the years.

Nonetheless, firms should expect that FINRA will review for compliance regarding these ongoing areas of focus, namely obligations related to suitability determinations, including with respect to recommendations relating to complex products, mutual fund and variable annuities share classes, as well as recommendations to use margin or execute trades in a margin account; outside business activities and private securities transactions; private placements; communications with the public; anti-money laundering (AML); best execution; fraud (including microcap fraud), insider trading and market manipulation; net capital and customer protection; trade and order reporting; data quality and governance; recordkeeping, risk management and supervision related to these and other areas.

In addition, FINRA will focus on risks related to associated persons with a problematic regulatory history.[1] Although this is a longstanding priority, we will continue to enhance our examination program to evaluate how firms address these risks in their hiring practices and supervision programs.[2]

FINRA will also continue to review the adequacy of firms' cybersecurity programs to protect sensitive information, including personally identifiable information. FINRA recently published our *Report on Selected Cybersecurity Practices – 2018*, and this document provides additional information on practices that may help some firms strengthen their cybersecurity programs.[3]

In addition, FINRA's *2017* and *2018 Reports on Examination Findings* present observations on concerns and effective practices relevant to many of the topics addressed in this letter, and FINRA encourages firms to use those reports, this letter and other resources FINRA makes available to enhance their compliance, supervisory and risk management programs.[4]

Highlighted Items

Online Distribution Platforms

Firms increasingly are involved in the distribution of securities through online platforms in reliance on Rule 506(c) of Regulation D and Regulation A under the Securities Act of 1933 (Securities Act). While some online distribution platforms are owned and operated by broker-dealers, others are operated by unregistered entities, which may use member firms as selling agents or brokers of record, or to perform activities such as custodial, escrow, back-office and financial technology (FinTech)-related functions.

FINRA is concerned that some member firms assert they are not selling or recommending securities when involved with online distribution platforms despite evidence to the contrary, including handling customer accounts and funds, or receiving transaction-based compensation. We will evaluate how firms conduct their reasonable basis and customer-specific suitability analyses, supervise communications with the public and meet AML requirements. Further, given the broad visibility of offerings distributed through online platforms, FINRA will evaluate how firms are addressing the risk of offering documents or communications with the public that omit material information or may contain false or misleading statements, or promissory claims of high targeted returns. For offerings subject to Regulation D, we will also evaluate how firms address the risk of sales to non-accredited investors and non-compliant escrow arrangements. For offerings subject to Regulation A, FINRA will also assess the risk of excessive or undisclosed compensation arrangements between firms and the issuers.

Fixed Income Mark-Up Disclosure

FINRA will review firms' compliance with their mark-up or mark-down disclosure obligations on fixed income transactions with customers pursuant to amendments to FINRA Rule 2232 (Customer Confirmations) and MSRB Rule G-15, which became effective on May 14, 2018.

To help firms evaluate their compliance with mark-up requirements, FINRA developed a Mark-up/Mark-down Analysis Report that is available to individual firms. The report provides a mark-up summary (including median and mean percentage mark-ups), detailed information such as trade details (*e.g.,* FINRA's calculated markup percentage and dollar profit) and graphical displays of data across longer periods of time for trend analysis. FINRA also made publicly available the Bond Facts Tool, which provides security-specific product data to help retail investors understand the quality of their fixed income securities transactions (*e.g.,* the time, price and size of other transactions in the same bond).

FINRA will also review for any changes in firms' behavior that might be undertaken to avoid their mark-up and mark-down disclosure obligations.

Regulatory Technology

Firms are using a variety of innovative regulatory technology (RegTech) tools to make their compliance efforts more efficient, effective and risk-based.[5] FINRA will engage with firms to understand how they are using such tools and addressing related risks, challenges or regulatory concerns, including those relating to supervision and governance systems, third-party vendor management, safeguarding customer data and cybersecurity.

Sales Practice Risks

Suitability

As always, suitability will remain one of FINRA's top priorities. This year, some of the specific areas on which we may focus include: (1) deficient quantitative suitability determinations or related supervisory controls; (2) overconcentration in illiquid securities, such as variable annuities, non-traded alternative investments and securities sold through private placements; and (3) recommendations to purchase share classes that are not in line with the customer's investment time horizon or hold for a period that is inconsistent with the security's performance characteristics (which could include, for example, a recommendation to purchase and hold a security that is intended for short-term trading or to engage in short-term trading in products designed primarily for long-term holding).

As the exchange-traded product (ETP) market continues to grow with novel and increasingly complex products, FINRA will evaluate whether firms are meeting their suitability obligations and risk disclosure obligations when recommending such products. These include leveraged and inverse exchange-traded funds (ETFs), floating-rate loan ETFs (also known as bank-loan or leveraged loan funds) and mutual funds that invest in loans extended to highly indebted companies of lower credit quality.

In addition, FINRA remains concerned about securities products that package leveraged loans (*e.g.,* collateralized loan obligations). Although these products are typically sold via private placement to qualified institutional buyers, if we observe that firms are selling them to retail investors, we will review how firms are supervising such transactions to ensure their compliance with applicable sales restrictions.

Senior Investors

Protection of senior investors, as well as investors who are retired or approaching retirement, remains a top priority for FINRA and we will continue to focus on how firms are protecting such persons from fraud, sales practice abuses and financial exploitation. FINRA will assess firms' supervision of accounts where registered representatives serve in a fiduciary capacity, including holding a power of attorney, acting as a trustee or co-trustee, or having some type of beneficiary relationship with a non-familial customer account. In particular, we are concerned about registered representatives using their role as a fiduciary to take control of trusts or other assets and direct funds to themselves.[6] FINRA will assess the supervisory systems firms employ to place heightened scrutiny over such accounts.

FINRA will also review firms' controls regarding their obligations under amendments to FINRA Rule 4512 (Customer Account Information) requiring firms to make reasonable efforts to obtain information about trusted contacts for non-institutional accounts and new FINRA Rule 2165 (Financial Exploitation of Specified Adults), to the extent that firms anticipate placing temporary holds on disbursements pursuant to the Rule 2165 safe harbor, including whether firms have clearly defined policies and procedures or practices.

FINRA is also interested in learning about firms' early experiences with these new provisions. FINRA developed them, in large measure, to provide firms with tools to protect seniors and other specified adults, which is especially important for firms that have, or soon will have, a significant number of customers who fall into such categories.[7]

Outside Business Activities and Private Securities Transactions

FINRA will continue to assess firms' controls related to associated persons' outside business activities[8] and private securities transactions, including associated persons raising funds from their customers away from their firm and outside of their firm's supervision. We are particularly concerned about fundraising activities for entities that the associated persons control or in which they have an interest, specifically entities with potentially misleading names that are similar to established issuers.

Operational Risks

Supervision of Digital Assets Business

Some firms have demonstrated significant interest in participating in activities related to digital assets and FINRA encourages firms to notify FINRA if they plan to engage in such activities, even where a membership application is not required.[9] This year, FINRA will review firms' activities through its membership and examination processes related to digital assets and assess firms' compliance with applicable securities laws and regulations and related supervisory, compliance and operational controls to mitigate the risks associated with such activities. Coordinating closely with the U.S. Securities and Exchange Commission, FINRA will consider how firms determine whether a particular digital asset is a security and whether firms have implemented adequate controls and supervision over compliance with rules related to the marketing, sale, execution, control, clearance, recordkeeping and valuation of digital assets, as well as AML/Bank Secrecy Act rules and regulations.

Customer Due Diligence and Suspicious Activity Reviews

FINRA will assess firms' compliance with FinCEN's Customer Due Diligence (CDD) rule, which became effective on May 11, 2018. The CDD rule requires that firms identify beneficial owners of legal entity customers, understand the nature and purpose of customer accounts, conduct ongoing monitoring of customer accounts to identify and report suspicious transactions and, on a risk basis, update customer information. FINRA will focus on the data integrity of those suspicious activity monitoring systems, as well as the decisions associated with changes to those systems.

Market Risks

Best Execution

FINRA is concerned about firms failing to use reasonable diligence to assure that their customer order flow is directed to the best market given the size and types of transactions, the terms and conditions of orders and other factors. In particular, FINRA will review firms' best execution decision-making where the firm routed all or substantially all customer orders to a small number of wholesale market makers from which they received payment for order flow or an affiliated broker-dealer or an

alternative trading system (ATS) in which the firm had a financial interest. FINRA will also assess how firms check additional venues for potential price improvement. FINRA will also review how firms quantify the benefits to customers from firms' receipt of order routing inducements and how firms manage the conflict of interest between their duty of best execution and any inducements or benefits they receive from the routing or internalization of customer orders.

Market Manipulation

FINRA continues to focus on market manipulation by enhancing FINRA's surveillance capabilities and providing firms with tools they can use to identify possible manipulative activities. This year, FINRA will focus on manipulative trading in correlated ETPs, including those that track common, broad market indices. We are using pattern exploration to better identify the exploitation of the unique characteristics of ETPs, such as the creation and redemption process and composition changes to the ETP portfolios, and expanding the use of machine learning to improve our ability to react to changes in the ETP market. Similarly, FINRA will focus on reviews for potential manipulation across correlated options products (*e.g.,* options on broad market indices and options on ETFs overlying the same indices).

FINRA will also continue to help firms with their compliance efforts by providing Cross Market Supervision Report Cards. These report cards help firms identify potential manipulation across multiple firms, markets and products and proactively address related compliance risks.

Market Access

FINRA will continue to review firms' compliance with Rule 15c3-5 (the Market Access Rule) under the Securities Exchange Act of 1934 (Exchange Act), focusing on how firms apply appropriate controls and limits to sponsored access orders; retain the sole authority to determine the boundaries for those controls and limits; test the effectiveness of those controls and limits; and implement and test exception reporting systems covering sponsored access orders. We will also assess how firms monitor their customers' activity and maintain policies and procedures, as well as technical controls, to detect and prevent potentially manipulative or other prohibited trading activity.

Short Sales

FINRA will review whether firms have structured their aggregation units in a manner that is consistent with the requirements of Exchange Act Rule 200(f) and can demonstrate the independence of the units through measures such as separate management structures, location, business purpose, and profit and loss treatment.

Short Tenders

As in 2018, FINRA will review how firms account for their options positions when tendering shares in the offer. Exchange Act Rule 14e-4 provides that if, following the announcement of a tender offer, a market participant sells call options with a strike price less than the tender offer price, the firm must reduce its long position by the shares underlying the options for purposes of calculating its net long position. FINRA will continue to educate firms about these requirements and evaluate their compliance with them.

Financial Risks

Credit Risk

FINRA will review firms' policies and procedures for identifying, measuring and managing credit risk, including risk exposures that may not be readily apparent. For example, a firm may be exposed to credit risk when it becomes responsible for transactions that its customers and correspondents execute "away" from the firm, without the firm's participation until after execution. Such responsibility can be incurred under clearing arrangements, prime brokerage arrangements (especially fixed income prime brokerage), "give up" arrangements, sponsored access arrangements (discussed above under "Market Access") or principal letters. Usually trades under these arrangements are completed without incident, but if they are sizable and conducted in a period of high volatility, they may create large exposures for which the firm holds little or no collateral (and which the firm may need to fund out of its own resources).

FINRA will also assess the extent to which firms identify and address all relevant risks when they extend credit to their customers and counterparties. Since broker-dealers generally extend secured credit, a firm may believe that its margin requirements eliminate counterparty or customer credit risk. A firm, however, can be exposed to sizeable losses in the event of a default by a customer whose margin account contains illiquid, volatile or concentrated securities positions because the firm may not be able to promptly liquidate the positions at a price that fully covers the customer's obligations. Similar risk exposures may exist when firms lend on products or strategies that have potential for large market moves, such as certain options strategies and structured products. In connection with this review, we will also examine firms' compliance with FINRA Rule 4210(f)(1) (Margin Requirements), which requires substantial additional margin on long and short positions in securities that are subject to "unusually rapid or violent changes in value, or do not have an active market on a national securities exchange, or where the amount carried is such that the position(s) cannot be liquidated promptly."

Funding and Liquidity

FINRA will continue to evaluate firms' liquidity planning, including whether they have a reasonable process to regularly assess the adequacy of their liquidity pools and update their stress test assumptions based on changes in their businesses, products and customers. This year, we will focus on whether firms update their stress test assumptions in light of changes in the marketplace, such as the increased volatility experienced at various points in 2018. Among other things, if government securities repo funding has a significant role in a firm's liquidity plan, we will inquire about the firm's contingency plans for disruptions of, or reductions in funding available from, the government securities repo market (which experienced significant quarter-end and year-end rate spikes in 2018). We will also assess the adequacy of firms' liquidity pools and their review of the reasonableness of stress test assumptions on a regular basis in light of all of their business activities and arrangements, including any arrangements where firms become responsible for transactions that their customers and correspondents execute "away" from them.

If you have general comments regarding this letter or suggestions on how we can improve it, please send them to Carlo di Florio, Executive Vice President, Member Supervision/Shared Services, at *carlo.diflorio@finra.org* or Steven Polansky, Senior Director, Member Supervision/Shared Services, at *steven.polansky@finra.org*.

Endnotes

1 FINRA uses "a risk model that takes into account a range of quantitative and qualitative information" to determine whether a registered representative poses additional risk to investors. Robert W. Cook, President and CEO, FINRA, Address at the McDonough School of Business, Georgetown University, Protecting Investors From Bad Actors (June 12, 2017). This information comes "from a variety of sources, including regulatory reports by firms and brokers, our examination program, employment histories, past associations with problematic firms, customer complaints, and any history of informal actions levied by FINRA" and FINRA also reviews "aggravating factors such as patterns of behavior, conflicts of interest, and links to previously disciplined individuals." *Id.*

2 *See Notice to Members 97-19* (providing certain hiring practices when considering for employment an associated person with a history of customer complaints, disciplinary actions or arbitrations from the securities industry); *Regulatory Notice 18-15* (listing the kinds of industry and regulatory-related incidents that firms should consider, and highlighting that statutorily disqualified persons and persons who have been disciplined in disciplinary proceedings raise significant investor protection concerns).

3 Firms can also find additional information about the main elements of a cybersecurity program in FINRA's Report on Cybersecurity Practices.

4 Resources that FINRA makes available to firms include, but are not limited to, the Small Firm Cybersecurity Checklist, the Anti-Money Laundering (AML) Template for Small Firms and the Report Center. For more information about these and other tools, please visit the Compliance Tools page on FINRA's website.

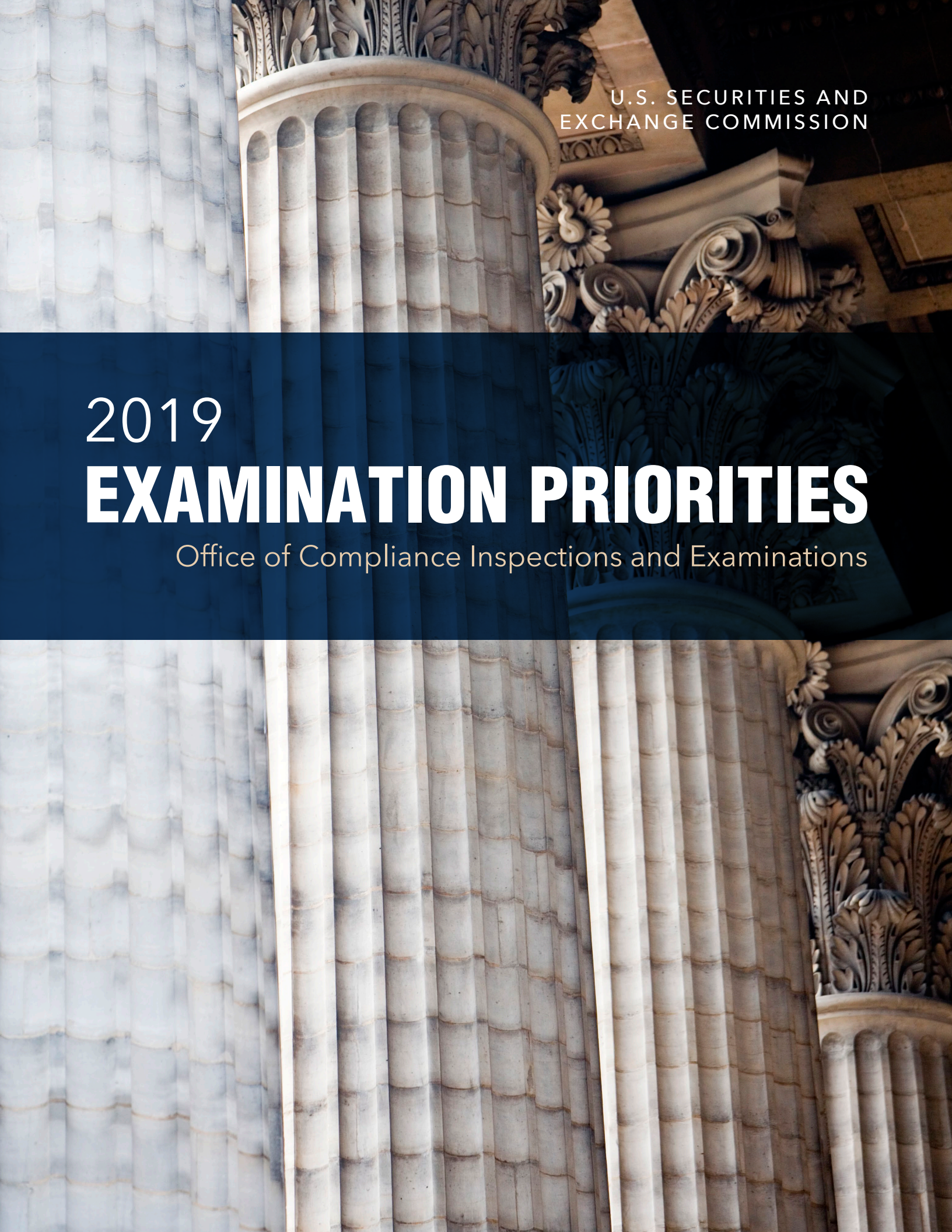
5 The term "RegTech" is generally used to refer to new and innovative technologies designed to facilitate firms' ability to meet their regulatory compliance obligations. *See* the Institute of International Finance defines RegTech as "the use of new technologies to solve regulatory and compliance burdens more effectively and efficiently." *See Technology Based Innovations for Regulatory Compliance ("RegTech") in the Securities Industry* (September 2018).

6 To the extent that the firm allows its registered representatives to engage in these fiduciary appointments for individuals who are not customers of the broker-dealer, firms should consider providing training to registered representatives that outlines or clarifies when the activity should be reported to the firm pursuant to FINRA Rule 3270 (Outside Business Activities of Registered Persons).

7 A "specified adult" under FINRA Rule 2165(a)(1) is defined as "(A) a natural person age 65 or older; or (B) a natural person age 18 or older who the member reasonably believes has a mental or physical impairment that renders the individual unable to protect his or her own interests." The "trusted contact" provision in Rule 4512 is intended to be a resource for a firm in administering a customer's account, protecting assets and responding to possible financial exploitation. *See Regulatory Notice 17-11* (noting that, in addition to responding to possible financial exploitation of seniors and other specified adults, a trusted contact could be helpful if a firm has been unable to contact a customer or there is concern over a customer's wellbeing).

8 Following a retrospective review of the outside business activities and private securities transactions rules, FINRA published *Regulatory Notice 18-08*, soliciting comment on proposed FINRA Rule 3290, which would replace current FINRA Rules 3270 (Outside Business Activities of Registered Persons) and 3280 (Private Securities Transactions of an Associated Person). FINRA received 52 comments on *Regulatory Notice 18-08* and they are available here. FINRA is considering the comments.

9 *See Regulatory Notice 18-20*.



U.S. SECURITIES AND EXCHANGE COMMISSION

2019

EXAMINATION PRIORITIES

Office of Compliance Inspections and Examinations

CONTENTS

MESSAGE FROM OCIE'S LEADERSHIP TEAM

The Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC) is pleased to announce its 2019 examination priorities.

With approximately 1,000 staff in the Commission's 11 regional offices and headquarters, OCIE is responsible for overseeing more than 13,200 investment advisers, approximately 10,000 mutual funds and exchange traded funds, roughly 3,800 broker-dealers, about 330 transfer agents, 7 active clearing agencies, 21 national securities exchanges, nearly 600 municipal advisors, the Financial Industry Regulatory Authority (FINRA), the Municipal Securities Rulemaking Board (MSRB), the Securities Investor Protection Corporation, and the Public Company Accounting Oversight Board.

OCIE completed over 3,150 examinations in Fiscal Year (FY) 2018, which is a 10 percent increase over FY 2017. Coverage of investment advisers increased to approximately 17 percent of SEC-registered investment advisers, up from approximately 15 percent in 2017. Examinations of investment companies were also up this year, increasing by approximately 45 percent. OCIE completed over 300 examinations of broker-dealers and actively oversaw FINRA and other regulated entities.

DID YOU KNOW?

OCIE's work stands on four "pillars": promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy.

The financial markets, products and services offered, and innovation in advanced technology continue to grow at a rapid pace. Operations of registered entities have also grown more complex, diverse, and interconnected, becoming more dependent on linkages to other organizations located throughout the world. In addition, the demands on OCIE's resources continue to grow with continued increases in the number of firms, particularly investment advisers registered with the SEC.

Over the past year, the number of registered investment advisers grew by nearly 5 percent, while the amount of assets managed by these advisers increased to approximately $84 trillion. The complexity of these advisers also continues to grow: more than 3,700 advisers have over one billion dollars in assets under management; approximately 35 percent manage a private fund; more than 50 percent have custody of client assets; more than 60 percent are affiliated with other financial industry firms; and approximately 12 percent provide advisory services to a mutual fund, exchange traded fund, or other registered investment company. For the broker-dealer community, despite the overall number of registered broker-dealers decreasing slightly, there were over 100 firms newly registered last year. Overall, broker-dealers operate more than 156,000 branch offices and approximately 10 percent of all broker-dealers are dually-registered with the SEC as investment advisers.

In 2019, OCIE will continue to stay abreast of changes in the SEC's registrant base, the markets, and investor needs and preferences, and will adjust its risk-based program in response to these changes. To this end, OCIE is increasingly leveraging technology and data analytics as well as human capital to fulfill its mission. This includes continually adding to and refining the expertise, tools, and applications that help identify areas of risk, firms that may present heightened risk of non-compliance, and activities that may harm investors.

The SEC's recently adopted Strategic Plan reiterated the importance of examinations. It described using examination resources to bolster regulatory requirements and protect investors as a "core principle" that the SEC has applied over the past 84 years to carry out its mission to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The SEC's Strategic Plan also is clear that future success requires the SEC to be efficient and nimble in the allocation of its resources. OCIE contributes to the fulfillment of the SEC's Strategic Plan by putting its limited resources to their highest and best use and performing high-quality, effective, efficient, and risk-targeted exams.

The priorities provide a preview of key areas where OCIE intends to focus its limited resources, but they do not encompass all of the areas that will be covered in examinations. To ensure the effective and efficient allocation of examination resources, OCIE proactively engages with registrants through outreach events, including national and regional compliance seminars. In FY 2018, OCIE staff participated in or held more than 100 such industry and regulatory outreach events.

OCIE also believes in the importance of engaging with senior leadership and boards of directors at registered entities. These efforts provide insight into evolving markets, including changes in risks to the markets and investors, market dynamics, and investor preferences. They also provide an opportunity to discuss with industry participants mission-related regulatory and market-impacting developments. The information obtained is also shared across the SEC through intra-agency working groups. These efforts have helped OCIE develop its risk-based approach and execute its examinations more effectively. The input received at these outreach and monitoring efforts were incorporated into the selection of the 2019 priorities.

OCIE measures performance in multiple ways and always against the backdrop of its four pillars: promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy. Through the over 3,150 examinations, joint initiatives, outreach events and other efforts in 2018, OCIE's five program areas—Investment Adviser/Investment Company, Broker-Dealer and Exchanges, Clearance and Settlement (OCS), FINRA and Securities Industry Oversight, and the Technology Controls Program (TCP)—have advanced each pillar to the benefit of retail investors and the markets.

Promoting Compliance

- In response to the areas of concern and weaknesses identified in deficiency letters, firms often revised compliance policies and procedures, changed business practices, clarified a regulatory filing, or otherwise enhanced their disclosures.
- OCIE continued to prioritize transparency to investors, registrants, and the broader financial industry regarding its exam observations. Information about common compliance issues identified during examinations helps firms evaluate their own compliance policies and procedures and better identify weaknesses and areas for improvement. To foster transparency, OCIE has published the following five risk alerts since the publication of the 2018 priorities:
  - » Most Frequent Best Execution Issues Cited in Adviser Exams
  - » Most Frequent Advisory Fee and Expense Compliance Issues Identified in Examinations of Investment Advisers
  - » Risk-Based Examination Initiatives Focused on Registered Investment Companies
  - » Investment Adviser Compliance Issues Related to the Cash Solicitation Rule
  - » Observations from Investment Adviser Examinations Relating to Electronic Messaging

- TCP issued a first-of-its-kind letter summarizing select examination findings from FYs 2016 and 2017 to entities subject to Regulation Systems Compliance and Integrity (Regulation SCI), a rule intended to help strengthen the technology infrastructure of the U.S. securities markets. The letter highlighted issues OCIE believes these entities would benefit from considering when assessing and improving cyber security, IT system resiliency, and technology-related policies and procedures.
- OCIE promoted compliance through thousands of investment adviser examinations as well as with staff discussions at the National Compliance Outreach Seminar for Investment Advisers and Investment Companies. At this outreach event, staff discussed a wide variety of topics, including program priorities, issues related to fees and expenses, portfolio management trends, cybersecurity, compliance, regulatory hot topics, and rulemaking.
- OCS promoted compliance during exams of Systemically Important Financial Market Utilities and other registered clearing agencies, identifying areas for improvement in governance, operational risk management, and public disclosure.

DID YOU KNOW?

In FY 2018, OCIE completed over 3,150 examinations—representing a 10 percent increase over FY 2017.

Preventing Fraud

- Examinations led to more than 160 enforcement referrals and resulted in firms returning more than $35 million to investors.
- OCIE conducted retail-targeted examinations of broker-dealers focused on preventing fraud, such as potential misappropriation and the sale of high risk securities by broker-dealers who may not conduct sufficient research into an investment and its appropriateness for a client.
- Examinations of investment advisers also aimed to prevent harm to retail investors, particularly seniors and those saving for retirement. For example, examinations identified advisers that selected or recommended more expensive mutual fund share classes for clients when lower cost share classes were available, and either failed to disclose or made inadequate disclosure about financial incentives they had to select or recommend the more expensive share classes. Examinations also identified compliance issues regarding advisory activities in branch offices, which resulted in enhancements to oversight practices.

Identifying and Monitoring Risk

- Examinations of firms required to comply with Regulation SCI, including the national securities exchanges, registered clearing agencies, FINRA, the MSRB, plan processors, and certain alternative trading systems (collectively, "SCI entities") identified many issues that, if left unresolved, could increase the risk of systems compromise or disruption at SCI entities and, in turn, increase risks to investors and the markets. Among other issues, certain SCI entities had insufficient policies and procedures related to: data loss prevention; vendor risk management; inventory management; and timely, consistent, and effective implementation of vendor-issued security patches. In addition, certain firms failed to report system disruptions or outages in a timely manner.
- Focused reviews of fixed income best execution obligations were conducted to identify and monitor risks, and examiners observed that many broker-dealers were not conducting sufficient reviews of execution quality to ensure that retail investors were receiving best execution.

- Investment adviser examinations identified emerging risks at advisers selling or recommending digital assets, such as concerns related to custody and safekeeping of investor assets, valuation, omitted or misleading disclosures regarding the complexities of the products and technology, and the risks of dramatic price volatility.

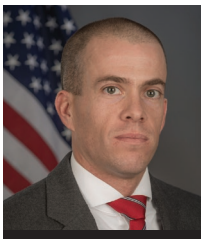
Informing Policy

- Examinations helped inform policy by providing further insight to other SEC Divisions and Offices regarding how registered entities have implemented the SEC's rules, the practical difficulties and challenges faced in complying with these rules, and common areas of non-compliance.
- Examinations into third party vendor management provided insight into, among other things, the use and management of cloud-based computing services.
- Examinations of compliance with the amended money market fund rules, disclosure relating to target fund glide path allocations, and fixed income cross trading practices provided valuable information about current practices in these areas.

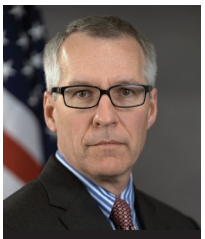
The Coming Year

- In 2019, many of OCIE's priorities have changed as new risks have emerged and existing risks have heightened or been mitigated. While priorities shift, OCIE's commitment to the SEC's mission and doing the utmost to protect investors and serve the American people will never change.

Peter B. Driscoll
Director



Keith E. Cassidy
National Technology Controls Program Director



Kevin W. Goodman
National FINRA and Securities Industry Oversight Director

Daniel R. Gregus
National Clearing Agency Director

Daniel S. Kahl
Co-Deputy Director, Chief Counsel

John S. Polise
National Broker Dealer and Exchange Director

James R. Reese
Chief Risk Officer

Kristin A. Snyder
Co-Deputy Director, National Investment Adviser/Investment Company Director

INTRODUCTION

In 2019, OCIE will prioritize certain practices, products, and services that it believes present potentially heightened risk to investors or the integrity of the U.S. capital markets. Designed to support the SEC's mission to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation, the six themes for OCIE's 2019 Examination Priorities, which include perennial risk areas and developing products and services, are:

1. Matters of importance to retail investors, including seniors and those saving for retirement;
2. Compliance and risk in registrants responsible for critical market infrastructure;
3. Select areas and programs of FINRA and MSRB;
4. Digital Assets;[1]
5. Cybersecurity; and
6. Anti-Money Laundering.

DID YOU KNOW?

In FY 2018, OCIE achieved examination coverage of approximately 17 percent of registered investment advisers, up from 9 percent just five years ago.

These priorities are not exhaustive and will not be the only issues OCIE addresses in its examinations, risk alerts, and investor and industry outreach. While the priorities drive many of OCIE's examinations, the scope of any examination is determined through a risk-based approach that includes analysis of the registrant's operations, products offered, and other factors. This risk-based approach often results in examinations that address key aspects of the SEC's regulatory oversight, such as the disclosure of services, fees, expenses, conflicts of interest for investment advisers, and trading and execution quality issues for broker-dealers.

OCIE's risk-based approach, both in selecting registered entities to examine and determining the scope of risk areas to examine, remains flexible in order to cover emerging and exigent risks to investors and the marketplace as they arise. OCIE is continually evaluating changes in market conditions, industry practices, and investor preferences to assess risks to both investors and the markets.

Although change may be continual, OCIE's analytic efforts and examinations remain firmly grounded in its four pillars: promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy.

1 Digital Assets include cryptocurrencies, coins, and tokens.

RETAIL INVESTORS, INCLUDING SENIORS AND THOSE SAVING FOR RETIREMENT

OCIE prioritizes the protection of retail investors, particularly seniors and those saving for retirement, and pursues examinations of firms that provide products and services to these investors.

DID YOU KNOW?

In FY 2018, OCIE held a national investment adviser/investment company compliance outreach program, a compliance outreach program for municipal advisors, and participated in more than a hundred other outreach events in order to promote and improve industry compliance.

In furtherance of OCIE's commitment to retail investors, examinations will focus on the following areas:

Fees and Expenses: Disclosure of the Costs of Investing

Every dollar an investor pays in fees and expenses is a dollar not invested. It is critically important that investors are provided with proper disclosures of the fees and expenses they pay for products and services and that financial professionals accurately calculate and charge fees in accordance with these disclosures. OCIE will continue to review fees charged to advisory accounts, ensuring that the fees are assessed in accordance with the client agreements and firm disclosures.

For these examinations, OCIE will select firms with practices or business models that may create increased risks of inadequately disclosed fees, expenses, or other charges. With respect to mutual fund share classes, OCIE will continue to evaluate financial incentives for financial professionals that may influence their selection of particular share classes. In addition, OCIE remains focused on investment advisers participating in wrap fee programs, which charge investors a single bundled fee for both advisory and brokerage services. Continued areas of interest include the adequacy of disclosures and brokerage practices.

Conflicts of Interest

As fiduciaries, investment advisers have a duty to act and provide advice in the best interests of their clients. Ensuring that investment advisers are acting in a manner consistent with their fiduciary duty and meeting their contractual obligations to their clients is paramount to maintaining investor confidence in the markets and investment professionals.

Conflicts of interest provide incentives for financial professionals to recommend certain types of products and services. Examinations will review policies and procedures addressing the following:

Use of Affiliated Service Providers and Products: Advisers in some cases utilize services or products provided by affiliated entities. These arrangements present conflicts of interest related to, among other areas, portfolio management practices and compensation arrangements. OCIE will examine such arrangements, focusing on the impact to clients and the related disclosures of conflicts of interest that may be present.

Securities-Backed Non-Purpose Loans and Lines of Credit: A non-purpose loan or line of credit allows borrowers to use the securities in their brokerage or advisory accounts as collateral to obtain a loan, the proceeds of which cannot be used for purchasing or trading securities. OCIE has observed that advisers, broker-dealers, and their employees receive certain financial incentives to recommend these products to clients and/or customers. OCIE will assess this practice to determine whether registrants are, among other things, adequately disclosing the risks to clients and any conflicts of interest presented by recommending these loans.[2]

Borrowing Funds from Clients: Borrowing funds from clients presents a number of conflicts of interest for an investment adviser. Where examiners observe this practice, emphasis will be on whether adequate disclosures, including the potentially poor or failing financial condition of the investment adviser, are made to the client and the investment adviser has acted consistently with these disclosures.

Senior Investors and Retirement Accounts and Products

OCIE will conduct examinations that review how broker-dealers oversee their interactions with senior investors, including their ability to identify financial exploitation of seniors. In examinations of investment advisers, OCIE will continue to review the services and products offered to seniors and those saving for retirement. These examinations will focus on, among other things, compliance programs of investment advisers, the appropriateness of certain investment recommendations to seniors, and the supervision by firms of their employees and independent representatives.

Portfolio Management and Trading

Reviewing portfolio management processes is an integral component to investment adviser examinations. OCIE will review firms' practices for executing investment transactions on behalf of clients, fairly allocating investment opportunities among clients, ensuring consistency of investments with the objectives obtained from clients, disclosing critical information to clients, and complying with other legal restrictions.

OCIE will also examine investment adviser portfolio recommendations to assess, among other things, whether investment or trading strategies of advisers are: (1) suitable for and in the best interests of investors based on their investment objectives and risk tolerance; (2) contrary to, or have drifted from, disclosures to investors; (3) venturing into new, risky investments or products without adequate risk disclosure; and (4) appropriately monitored for attendant risks.

Never-Before or Not Recently-Examined Investment Advisers

OCIE will continue to conduct risk-based examinations of certain investment advisers that have never been examined, including newly-registered investment advisers as well as those registered for several years but that have yet to be examined. OCIE will also prioritize examinations of certain investment advisers that have not been examined for a number of years and may have substantially grown or changed business models.

2 See Investor Alert: Securities-Backed Lines of Credit, issued by the SEC's Office of Investor Education and Advocacy and FINRA, available at https://www.sec.gov/oiea/investor-alerts-bulletins/sbloc.html.

Mutual Funds and Exchange Traded Funds

Mutual funds and exchange traded funds (ETFs) are the primary investment vehicles for many retail investors. OCIE will continue to prioritize examinations of these funds, the activities of their advisers, and oversight practices of their boards of directors. Examinations will assess industry practices and regulatory compliance in various areas that may have significant impact on retail investors.

OCIE will focus on risks associated with the following: (1) index funds that track custom-built or bespoke indexes; (2) ETFs with little secondary market trading volume and smaller assets under management; (3) funds with higher allocations to certain securitized assets; (4) funds with aberrational underperformance relative to their peer groups; (5) funds managed by advisers that are relatively new to managing Registered Investment Companies (RICs); and (6) advisers that provide advice to both RICs and private funds with similar investment strategies.

Municipal Advisors

Municipal advisors (MAs) provide advice to, or on behalf of, a municipal entity with respect to the issuance of municipal securities or municipal financial products. OCIE will continue to conduct select examinations of MAs that have never been examined, concentrating on whether these MAs have satisfied their registration requirements and professional qualifications as well as continuing education requirements. OCIE will also prioritize whether MAs provided the appropriate disclosures regarding their conflicts of interests or otherwise violated their fiduciary duty to a municipal entity. Examinations will also review for compliance with recently-effective MSRB rules, including those relating to advertisements by MAs and the standards of conduct for MAs obtaining CUSIP numbers on behalf of issuers.

DID YOU KNOW?

Broker-dealers operate more than 156,000 branch offices, and approximately 10 percent of all broker-dealers are dually registered with the SEC as investment advisers.

Broker-Dealers Entrusted with Customer Assets

Broker-dealers that hold customer cash and securities must abide by certain rules, including the Customer Protection Rule (Exchange Act Rule 15c3-3), and have a significant responsibility to ensure that those assets are safeguarded and accurately reported. The Customer Protection Rule restricts the use of customer assets and prevents the broker-dealer from using customer assets as working capital. Examinations of select broker-dealers will focus on compliance with this rule, as well as procedures and controls to promote compliance.

Microcap Securities

OCIE will continue examinations of broker-dealers involved in selling stocks of companies with a market capitalization of under $250 million. OCIE will look at a variety of areas, including reviewing for manipulative schemes (i.e., pump and dump schemes), compliance with Regulation SHO, which governs short sales, and compliance with Exchange Act Rule 15c2-11, which governs the submission and publication of quotations by broker-dealers for certain over-the-counter equity securities.

COMPLIANCE AND RISK IN REGISTRANTS RESPONSIBLE FOR CRITICAL MARKET INFRASTRUCTURE

Clearing Agencies

Clearing agencies promote market stability and efficiency and help to reduce risk by performing critical post trade services, including acting as intermediaries between and guarantors for buyers and sellers of securities, facilitating the settlement of investor trades, and acting as a depository for securities and other financial instruments. For example, clearing agencies may reconcile transaction information received from the parties to a trade, calculate settlement obligations, or hold securities as certificates or in electronic form to facilitate automated settlement. As a result, clearing agencies help ensure that trades settle on time and at the agreed upon terms.

DID YOU KNOW?

Clearing agencies perform a variety of services that help ensure trades settle on time and at the agreed upon terms.

OCIE will continue to conduct annual examinations of clearing agencies that the Financial Stability Oversight Council has designated as systemically important and for which, under the Dodd- Frank Act, the Commission is the supervisory agency. OCIE will also conduct risk-based examinations of other registered clearing agencies. Examinations will focus on: (1) compliance with the SEC's Standards for Covered Clearing Agencies and other federal securities laws applicable to registered clearing agencies; (2) whether clearing agencies have taken timely corrective action in response to prior examinations; and (3) other areas identified in collaboration with the SEC's Division of Trading and Markets and with other regulators.

Entities Subject to Regulation Systems Compliance and Integrity

Regulation SCI was adopted by the Commission to strengthen the technology infrastructure of the U.S. securities markets. Among other things, it requires SCI entities to establish, maintain, and enforce policies and procedures designed to ensure that their systems' capacity, integrity, resiliency, availability, and security are adequate to maintain their operational capability and promote the maintenance of fair and orderly markets. If certain events occur, these entities are required to take corrective action as soon as reasonably practical and immediately notify the SEC of the occurrence.

OCIE will continue to examine SCI entities to evaluate whether they have effectively implemented written policies and procedures required by Regulation SCI. OCIE will also focus on, among other things, controls relating to software development life cycles and related governance procedures, effectiveness of internal audit programs, inventory management, and threat management capabilities.

Transfer Agents

Transfer agents serve as agents for securities issuers and play a critical role in the settlement of securities transactions. Among their key functions, transfer agents are responsible for maintaining issuers' securityholder records, recording changes of ownership, canceling and issuing certificates, distributing dividends and other payments to securityholders, and facilitating communications between issuers and securityholders. Efficient transfer agent operations are critical to secondary securities markets and for recordkeeping during primary market activities. Examinations will assess transfers, recordkeeping, and the safeguarding of funds and securities. Examinations will also focus on the requirement for transfer agents to annually file a report by an independent accountant concerning the transfer agency's system of internal accounting controls.

Examination candidates will include transfer agents that serve as paying agents for issuers, transfer agents developing blockchain technology, or transfer agents that provide services to issuers of microcap securities, private offerings, crowdfunded securities, or digital assets.

National Securities Exchanges

With over 20 national securities exchanges facilitating transactions in the marketplace, OCIE will examine internal audit and surveillance programs and funding for regulatory programs.

FOCUS ON FINRA AND MSRB

FINRA

FINRA is a registered national securities association that adopts and enforces rules governing the conduct of its members. These members are also registered with the SEC as broker-dealers. FINRA oversees approximately 3,800 brokerage firms, 156,000 branch offices, and 630,000 registered representatives through examinations, enforcement, and surveillance. In addition, FINRA, among other things, provides a forum for securities arbitration and mediation, conducts market regulation, including by contract for a majority of national securities exchanges, reviews broker-dealer advertisements, administers the testing and licensing of registered persons, and operates industry utilities such as Trade Reporting Facilities. Examinations of FINRA will continue to focus on FINRA's operations and regulatory programs and the quality of FINRA's examinations of broker-dealers and municipal advisors that are also registered as broker-dealers.

DID YOU KNOW?

FINRA oversees approximately 3,800 brokerage firms, 156,000 branch offices, and 630,000 registered representatives through examinations, enforcement, and surveillance.

MSRB

MSRB regulates the activities of broker-dealers that buy, sell, and underwrite municipal securities, and municipal advisors. MSRB establishes rules for municipal securities dealers and municipal advisors, supports market transparency by making municipal securities trade data and disclosure documents available, and conducts education and outreach regarding the municipal securities market. OCIE, in coordination with FINRA, conducts examinations of MSRB members to ensure compliance with MSRB rules. Given MSRB's broad responsibility to regulate municipal securities transactions, OCIE will continue to conduct inspections of MSRB to evaluate the effectiveness of MSRB's policies, procedures, and controls.

DIGITAL ASSETS

The digital asset market has grown rapidly and may present risks to retail investors. The number of digital asset market participants, including broker-dealers, trading platforms, and investment advisers, also continues to increase. Given the significant growth and risks presented in this market, OCIE will continue to monitor the offer and sale, trading, and management of digital assets, and where the products are securities, examine for regulatory compliance. In particular, through high level inquiries, OCIE will take steps to identify market participants offering, selling, trading, and managing these products or considering or actively seeking to offer these products and then assess the extent of their activities. For firms actively engaged in the digital asset market, OCIE will conduct examinations focused on, among other things, portfolio management of digital assets, trading, safety of client funds and assets, pricing of client portfolios, compliance, and internal controls.

CYBERSECURITY

Cybersecurity protection is critical to the operation of the financial markets. The impact of a successful cyber-attack may have consequences that extend beyond the firm compromised to other market participants and retail investors, who may not be well informed of these risks and consequences. OCIE is working with firms to identify and manage cybersecurity risks and to encourage market participants to actively and effectively engage in this effort.

OCIE will continue to prioritize cybersecurity in each of its five examination programs. Examinations will focus on, among other things, proper configuration of network storage devices, information security governance generally, and policies and procedures related to retail trading information security. Specific to investment advisers, OCIE will emphasize cybersecurity practices at investment advisers with multiple branch offices, including those that have recently merged with other investment advisers, and continue to focus on, among other areas, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

ANTI-MONEY LAUNDERING PROGRAMS

The Bank Secrecy Act requires broker-dealers to establish anti-money laundering (AML) programs. These programs must, among other things, include policies and procedures reasonably designed to identify customers, perform customer due diligence, monitor for suspicious activity, and where appropriate, file suspicious activity reports (SARs) with the Financial Crimes Enforcement Network. SARs are used to detect and combat terrorist financing, public corruption, market manipulation, and a variety of other fraudulent behavior.

In 2019, OCIE will continue to prioritize examining broker-dealers for compliance with their AML obligations, including whether they are meeting their SAR filing obligations, implementing all elements of their AML program, and robustly and timely conducting independent tests of their AML program. The goal of these examinations is to ensure that broker-dealers have policies and procedures in place that are reasonably designed to identify suspicious activity and illegal money laundering activities.

CONCLUSION

These priorities reflect OCIE's assessment of certain risks, issues, and policy matters arising from market and regulatory developments, information gathered from examinations, and other sources, including tips, complaints, and referrals, and coordination with other regulators. OCIE welcomes comments and suggestions regarding how it can better fulfill its mission to promote compliance, prevent fraud, identify and monitor risk, and inform SEC policy. OCIE's contact information is available at https://www.sec.gov/ocie/ocie_org.htm. If you suspect or observe activity that may violate the federal securities laws or otherwise operates to harm investors, please notify SEC staff at https://www.sec.gov/tcr.

U.S. Securities and
Exchange Commission
100 F Street NE
Washington, DC 20549
SEC.gov

NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations[*]

Observations from Investment Adviser Examinations Relating to Electronic Messaging

I. Introduction

Key takeaway. *OCIE encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with applicable regulatory requirements.*

The Office of Compliance Inspections and Examinations ("OCIE") conducted a limited-scope examination initiative of registered investment advisers ("advisers") designed to obtain an understanding of the various forms of electronic messaging used by advisers and their personnel, the risks of such use, and the challenges in complying with certain provisions of the Investment Advisers Act of 1940 ("Advisers Act"). OCIE conducted this initiative because it noticed an increasing use of various types of electronic messaging by adviser personnel for business-related communications.[1]

The purpose of this Risk Alert is to remind advisers of their obligations when their personnel use electronic messaging and to help advisers improve their systems, policies, and procedures by sharing the staff's observations from these examinations.

II. Relevant Regulation

Advisers Act Rule 204-2 ("Books and Records Rule") requires advisers to make and keep certain books and records relating to their investment advisory business, including typical accounting and other business records as required by the Commission. For example, Rule 204-2(a)(7) requires advisers to make and keep "[o]riginals of all written communications received and copies of all written communications sent by such investment adviser relating to (i) any recommendation made or proposed to be made and any advice given or proposed to be given, (ii) any receipt, disbursement or delivery of funds or securities, (iii) the placing or execution of any order to purchase or sell any security, or (iv) the performance or rate of return of any or all managed accounts or securities recommendations," subject to certain limited exceptions.

Additionally, Rule 204-2(a)(11) requires advisers to make and keep a copy of each notice,

[*] The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (the "SEC" or the "Commission") has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

[1] Numerous articles also have been written on electronic messaging trends and the compliance challenges that they may pose. *See e.g.*, Jackie Noblett, *SMH: Texting, Chat Continue to Vex Compliance Depts.*, IGNITES (June 2, 2017) and Jason Wallace, *Text Messaging: The Communication Risk Compliance Fears Most – Survey*, REGULATORY INTELLIGENCE (May 26, 2017).

circular, advertisement, newspaper article, investment letter, bulletin or other communication that the investment adviser circulates or distributes, directly or indirectly, to ten or more persons. The Commission has stated that, "regardless of whether information is delivered in paper or electronic form, broker-dealers and investment advisers must reasonably supervise firm personnel with a view to preventing violations."[2]

Advisers Act Rule 206(4)-7 ("Compliance Rule") requires advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and rules thereunder.[3] According to the Compliance Rule's adopting release, each adviser should identify compliance factors creating risk exposures for the firm and its clients in light of the adviser's particular operations, and then design policies and procedures that address those risks.[4] The Commission stated that an adviser's policies and procedures should address, to the extent relevant to the adviser, "[t]he accurate creation of required records and their maintenance in a manner that secures them from unauthorized alteration or use and protects them from untimely destruction," among other things.[5] The Compliance Rule also requires an adviser to review, no less frequently than annually, the adequacy of the adviser's compliance policies and procedures and the effectiveness of their implementation.

As discussed below, a number of changes in the way mobile and personally owned devices are used pose challenges for advisers in meeting their obligations under the Books and Records Rule and the Compliance Rule.[6] These changes include the increasing use of social media, texting, and other types of electronic messaging apps, and the pervasive use of mobile and personally owned devices for business purposes.

III. Scope of Electronic Messaging Covered by the Examinations

OCIE's examinations surveyed firms to learn the types of electronic messaging used by firms and their personnel,[7] and reviewed firms' policies and procedures to understand how advisers were addressing the risks presented by evolving forms of electronic communication. For purposes of this initiative, "electronic messaging" or "electronic communication" included

---

[2] *Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information*, Advisers Act Rel. No. 1562 (May 9, 1996), *available at* https://www.sec.gov/rules/interp/33-7288.txt.

[3] Advisers Act Rule 206(4)-7(a).

[4] *Compliance Programs of Investment Companies and Investment Advisers*, Advisers Act Release No. 2204 (Dec. 17, 2003) at Section II.A.1., *available at* http://www.sec.gov/rules/final/ia-2204.htm.

[5] *See id.* at n.19 and accompanying text.

[6] This Risk Alert is not intended to be a comprehensive overview of all applicable regulatory requirements. The use of electronic messaging may implicate regulations beyond those specifically discussed in this Risk Alert.

[7] Adviser legal and regulatory requirements generally cover persons associated with an adviser, which can include many types of advisory personnel – such as employees, independent contractors, and investment adviser representatives. For purposes of this Risk Alert, the terms "personnel," "employees," and "representatives" are used interchangeably and include independent contractors.

written business communications conveyed electronically using, for example, text/SMS messaging, instant messaging, personal email, and personal or private messaging. OCIE included communications when conducted on the adviser's systems or third-party applications ("apps") or platforms or sent using the adviser's computers, mobile devices issued by advisory firms, or personally owned computers or mobile devices used by the adviser's personnel for the adviser's business.

The staff specifically excluded email use on advisers' systems from this review because firms have had decades of experience complying with regulatory requirements with respect to firm email, and it often does not pose similar challenges as other electronic communication methods because it occurs on firm systems and not on third-party apps or platforms.

IV. Summary of Examination Observations

OCIE's examination initiative focused on whether and to what extent advisers complied with the Books and Records Rule and adopted and implemented policies and procedures as required by the Compliance Rule. During the course of the initiative, the staff observed a range of practices with respect to electronic communications, including advisers that did not conduct any testing or monitoring to ensure compliance with firm policies and procedures. The staff observed and identified the following examples of practices[8] that the staff believes may assist advisers in meeting their record retention obligations under the Books and Records Rule and their implementation and design of policies and procedures under the Compliance Rule:

Policies and Procedures

- Permitting only those forms of electronic communication for business purposes that the adviser determines can be used in compliance with the books and records requirements of the Advisers Act.
- Specifically prohibiting business use of apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up.
- In the event that an employee receives an electronic message using a form of communication prohibited by the firm for business purposes, requiring in firm procedures that the employee move those messages to another electronic system that the adviser determines can be used in compliance with its books and records obligations, and including specific instructions to employees on how to do so.
- Where advisers permit the use of personally owned mobile devices for business purposes, adopting and implementing policies and procedures addressing such use

[8] This Risk Alert is not intended to be a comprehensive list of practices for a firm to meet its regulatory obligations, but rather to provide a sample of practices staff observed that may be helpful to advisers assessing their compliance policies and procedures addressing electronic messaging, including with respect to recordkeeping, supervision, or cybersecurity.

with respect to, for example, social media, instant messaging, texting, personal email, personal websites, and information security.

- If advisers permit their personnel to use social media, personal email accounts, or personal websites for business purposes, adopting and implementing policies and procedures for the monitoring, review, and retention of such electronic communications.

- Including a statement in policies and procedures informing employees that violations may result in discipline or dismissal.

Employee Training and Attestations

- Requiring personnel to complete training on the adviser's policies and procedures regarding prohibitions and limitations placed on the use of electronic messaging and electronic apps and the adviser's disciplinary consequences of violating these procedures.

- Obtaining attestations from personnel at the commencement of employment with the adviser and regularly thereafter that employees (i) have completed all of the required training on electronic messaging, (ii) have complied with all such requirements, and (iii) commit to do so in the future.

- Providing regular reminders to employees of what is permitted and prohibited under the adviser's policies and procedures with respect to electronic messaging.

- Soliciting feedback from personnel as to what forms of messaging are requested by clients and service providers in order for the adviser to assess their risks and how those forms of communication may be incorporated into the adviser's policies.

Supervisory Review

- For advisers that permit use of social media, personal email, or personal websites for business purposes, contracting with software vendors to (i) monitor the social media posts, emails, or websites, (ii) archive such business communications to ensure compliance with record retention rules, and (iii) ensure that they have the capability to identify any changes to content and compare postings to a lexicon of key words and phrases.

- Regularly reviewing popular social media sites to identify if employees are using the media in a way not permitted by the adviser's policies. Such policies included prohibitions on using personal social media for business purposes or using it outside of the vendor services the adviser uses for monitoring and record retention.

- Running regular Internet searches or setting up automated alerts to notify the adviser when an employee's name or the adviser's name appears on a website to identify potentially unauthorized advisory business being conducted online.

- Establishing a reporting program or other confidential means by which employees can report concerns about a colleague's electronic messaging, website, or use of social media for business communications. Particularly with respect to social media, colleagues may be "connected" or "friends" with each other and see questionable or impermissible posts before compliance staff notes them during any monitoring.

Control over Devices

- Requiring employees to obtain prior approval from the adviser's information technology or compliance staff before they are able to access firm email servers or other business applications from personally owned devices. This may help advisers understand each employee's use of mobile devices to engage in advisory activities.

- Loading certain security apps or other software on company-issued or personally owned devices prior to allowing them to be used for business communications. Software is available that enables advisers to (i) "push" mandatory cybersecurity patches to the devices to better protect the devices from hacking or malware, (ii) monitor for prohibited apps, and (iii) "wipe" the device of all locally stored information if the device were lost or stolen.

- Allowing employees to access the adviser's email servers or other business applications only by virtual private networks or other security apps to segregate remote activity to help protect the adviser's servers from hackers or malware.

V. Conclusion

In sharing its observations from this examination initiative, OCIE encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with their regulatory requirements. OCIE also encourages advisers to stay abreast of evolving technology and how they are meeting their regulatory requirements while utilizing new technology.

While this initiative was limited to examinations of investment advisers and this Risk Alert only references regulatory provisions under the Advisers Act, other types of regulated financial services entities may face similar challenges with new communication tools and methods.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

Report on Selected Cybersecurity Practices – 2018

DECEMBER 2018

Contents

A REPORT FROM **THE FINANCIAL INDUSTRY REGULATORY AUTHORITY**

Introduction

This report continues FINRA's efforts to share information that can help broker-dealer firms further develop their cybersecurity programs. Firms routinely identify cybersecurity as one of their primary operational risks. Similarly, FINRA continues to see problematic cybersecurity practices in its examination and risk monitoring program. This report presents FINRA's observations regarding effective practices that firms have implemented to address selected cybersecurity risks while recognizing that there is no one-size-fits-all approach to cybersecurity.

When selecting the topics for this report, FINRA considered the evolving cybersecurity threat landscape, firms' primary challenges and the most frequent cybersecurity findings from our firm examination program. First, we address how firms have strengthened their cybersecurity controls in branch offices, which is especially important for firms with decentralized business models. Second, we discuss limiting phishing attacks, which remain a top cybersecurity challenge for many firms. Third, we explain the importance of identifying and mitigating insider threats, which are of concern for many firms. Fourth, we describe the elements of a strong penetration testing program. Finally, we share observations regarding establishing and maintaining controls on mobile devices, which have emerged as a significant risk for many firms because of their increasingly widespread use by employees and customers.

FINRA notes that the specific practices highlighted in this report should be evaluated in the context of a holistic firm-level cybersecurity program. FINRA's 2015 *Report on Cybersecurity Practices* addresses the elements of such cybersecurity programs and provides guidance to firms seeking to improve their current protocols. Further, small firms seeking to develop or improve their cybersecurity practices should review the appendix to this report "Core Cybersecurity Controls for Small Firms." This appendix, combined with the FINRA *Small Firm Cybersecurity Checklist* will assist small firms in identifying possible cybersecurity controls.

This report is not intended to express any legal position, and does not create any new legal requirements or change any existing regulatory obligations.

Inquiries regarding this report may be directed to Carlo di Florio, Executive Vice President, Member Supervision/Shared Services, at (212) 858-3908 or *carlo.diflorio@finra.org*; or Steven Polansky, Senior Director, Member Supervision/Shared Services, at (202) 728-8331 or *steven.polansky@finra.org*.

Branch Controls

FINRA has observed that some firms face challenges maintaining effective cybersecurity controls at their branch locations. Branches' autonomy from the home office may adversely affect firms' ability to implement a consistent firm-wide cybersecurity program. Some firms may experience increased challenges if their branches may, for example, purchase their own assets, use non-approved vendors or not follow their firms' software patching and upgrade protocols. Similarly, representatives working from home may require even further oversight and technological support to comply with firm standards. As a result, firms should evaluate whether they need to enhance their branch-focused cybersecurity measures to maintain robust cybersecurity controls and protect customer information across their organizations.

FINRA has observed firms implementing the following effective practices:

- Establishing Written Supervisory Procedures (WSPs) to define minimum cybersecurity controls for branches and formalize oversight of branch offices;
- Developing an inventory of branch-level data, software and hardware assets;
- Maintaining branch technical controls; and
- Implementing a robust branch cybersecurity examination program.

Branch-Level WSPs

Although most firms have developed WSPs addressing cybersecurity controls, FINRA has observed that branch offices may have less developed cybersecurity controls in comparison to the home office. In some cases, for example, firms may have distributed guidance on cybersecurity to branches in a range of memos, newsletters, questionnaires and training, but may not have consolidated those into a comprehensive, easily referenced set of minimum standards or best practices for their branches.[1] Other firms may not have formalized their oversight of branch offices' administration of cybersecurity controls.

FINRA has observed firms implementing the following effective practices:

- Developing branch-level WSPs and other comprehensive guidance on cybersecurity controls and distributing such guidance to all branches;
- Distributing alerts and notifications on emerging cybersecurity issues to both home office employees and branch representatives;
- Designating the branch office supervisor or another branch office staff member with responsibility for that branch's cybersecurity controls;
- Providing branches a list of required and recommended hardware and software options and settings, as well as approved vendors;
- Mandating that branch personnel notify branch management of and properly respond to violations of firm cybersecurity standards or material cybersecurity incidents involving loss of confidentiality, availability or integrity of customer personally identifiable information (PII) or sensitive firm data (*see* Sections 11 and 12 of FINRA's *Small Firm Cybersecurity Checklist*); and
- Mandating that registered representatives complete an annual attestation to comply with the firm's WSP requirements, including its cybersecurity policies.

Further, FINRA notes that training plays an integral role in improving the quality of branch-level cybersecurity programs and controls. In particular, firms could consider requiring branch staff and registered representatives with access to customer information, as well as those working remotely, to complete initial onboarding, as well as ongoing, regular training on firm cybersecurity standards, practices and risks (in addition to their required firm continuing education (CE) program training).[2] Ongoing training may include web-based or in-person courses, simulations of actual cases experienced by the firm or peer firms, security awareness bulletins and phishing or other campaigns. In order to determine the scope and depth of branch personnel training, firms may also consider incorporating into their training program a formal or informal evaluation of the staff's understanding of and compliance with firm cybersecurity requirements. *See* Section 8 of FINRA's *Small Firm Cybersecurity Checklist* for additional guidance on firm training.

Asset Inventory

Asset inventories are a key element of any firm's cybersecurity program, especially where branches' autonomy may make it difficult for firms to know the scope of assets they need to protect. Branches and registered representatives may not be aware of the locations where they store sensitive customer or firm data; use unapproved software, hardware or vendor-provided services; or not comply with other firm cybersecurity standards. An asset inventory can help reduce these risks and provide important information for managing branch office security controls.

When used in conjunction with a cybersecurity risk assessment, an asset inventory can serve as a starting point to identify critical assets and their vulnerability to attack, as well as appropriate policy, technical and physical controls to mitigate those risks.

For further information on asset inventories, see Sections 1 and 8 of FINRA's *Small Firm Cybersecurity Checklist* and the "Asset Inventories and Critical Assets" discussion in FINRA's *Report on Cybersecurity Practices*.

FINRA has observed firms implementing the following effective practices:

- Requiring branches to perform initial and recurring inventories of branch assets and update the firm regarding any changes;
- Identifying sensitive customer and firm information and the location(s) where such information is stored;
- Ensuring the physical security of branch assets;
- Establishing processes by which branches manage and report lost or stolen assets;
- Providing secured asset disposal, such as destroying hard drives of computers no longer in use; and
- Ensuring branch operating systems are properly supported and maintained either by the firm or by vendors.

Technical Controls

Firms face a variety of potential threats to their data and systems at the branch level. Firms can use a cybersecurity risk assessment to determine which threats are most significant for each branch and, then, identify and implement appropriate technical (and other) controls to mitigate those threats.[3]

FINRA has observed firms implementing the following effective practices:

- Developing identity and access management protocols for registered representatives and other staff, including managing the granting, maintenance and termination of access to firm and customer data;
- Limiting registered representatives' access to only their own customers' data and related exception reports;
- Setting minimum password requirements and multi-factor authentication for access to firm systems and applications by firm employees, registered representatives, vendors, contractors and other insiders (*see* Insider Threats section of this report, below);
- Prohibiting the sharing of passwords among firm staff;
- Prohibiting the storage of sensitive customer or firm data in unapproved or prohibited locations (*e.g.*, a file server, cloud provider or thumb drive and without encryption or transmitted without encryption);
- Establishing minimum encryption standards for all branch hardware used to access firm systems, including laptops, desktops, servers, mobile devices and removable media devices;
- Requiring branches to adhere to minimum encryption standards (and providing technical tools to enforce that standard) for data-in-transit, such as emails and file transfers that include customer PII or sensitive information;
- Ensuring branches use only secure, encrypted wireless settings for office and home networks;
- Maintaining regular patching, anti-virus protection, anti-malware and operating system updates for all branch computers and servers that access firm data in a manner that is consistent with firm, vendor and industry standards;
- Developing physical security protocols for all portable devices used to access firm data and systems, including laptops and mobile devices;
- Mandating all branch vendors (including cloud providers) meet firm security requirements, especially if firm data or other sensitive information will be accessed or maintained by the vendor; and
- Creating processes and selecting firm-approved vendors for the secure disposal of hard copy records and firm computer hardware (*e.g.*, hardware listed in the firm's inventory) that may contain sensitive information.

For further information on technical controls, see Sections 3 through 10 of FINRA's *Small Firm Cybersecurity Checklist* and FINRA's *Report on Cybersecurity Practices*.

Branch Review Program

Firms' branch office reviews are an important tool to evaluate branches' cybersecurity vulnerabilities and ensure that branches are consistently applying cybersecurity controls across a firm's branch network. The review program may include on-site branch inspections, remote surveillance, inspections, reports and questionnaires to evaluate and record each branch's and registered representative's compliance with the firm's cybersecurity standards.

FINRA has observed firms implementing the following effective practices:

- Developing a framework to capture cybersecurity risks, risk levels and related controls at each branch;
- Implementing periodic exam visits or risk-based audits, the frequency and focus of which may depend on the risk profile of each branch;
- Implementing automated ways to verify and monitor branch controls, such as verifying patching, virus and malware protection, encryption and password protection;
- Ensuring that firm branch examiners have sufficient cybersecurity expertise to perform effective examinations of branch cybersecurity programs;
- Confirming branches meet firm cybersecurity standards and use firm-recommended vendors or other vendors meeting firm standards;
- Imposing consequences (including but not limited to fines, sanctions, or termination) for branches and registered representatives engaging in repeat violations of firm standards;
- Providing compliance and technology support to branches and registered representatives implementing firm cybersecurity protocols; and
- Re-evaluating branches where branch reviews identified material deficiencies or reported material cybersecurity incidents to ensure that the branch has implemented corrective action.

Phishing

Social engineering or "phishing" attacks are one of the most common cybersecurity threats firms have discussed with FINRA. Phishing attacks may take a variety of forms, but all of them try to convince the recipient to provide information or take an action. Although some phishing emails are distributed to millions of recipients, other attempts are thoroughly researched and carefully customized to reach one or more selected individuals (*e.g.*, an individual who attackers have determined is likely to have administrator privileges), while a related attack targets one or more senior firm personnel (*e.g.*, the CEO or CFO). (These types of attacks are referred to as "spear phishing" and "whaling" respectively, but we refer to them collectively as "phishing" in the remainder of this document.)

In a phishing event, the attackers try to disguise themselves as a trustworthy entity or individual via email, instant message, phone call or other communication, where they request PII (such as Social Security numbers, usernames or passwords), direct the recipient to click on a malicious link, open an infected attachment or application or attempt to initiate a fraudulent wire transfer. Such "phishes" can appear to come from a variety of sources, including the following types of senders:

Entities	Individuals
Firm or affiliate	Friends
Government agencies, such as the U.S. Securities and Exchange Commission, FINRA and IRS	Customers
Banks or other financial institutions	Information Technology (IT) administrators or Help Desk representatives
Social media sites	Office managers
Auction sites	Senior executives
Online payment processors	CEO or CFO

The growing sophistication and quality of phishing (especially spear phishing and whaling) attacks makes it challenging for recipients to distinguish them from legitimate communications. The following list may help firms understand the hallmarks of phishing communication:

Category	Characteristics
Sender	Discrepancies between the name and email address or "reply to" address of the sender
	Unknown individual or corporation
	New individual with whom you do not regularly correspond, such as IT manager, senior manager or CEO of the organization
Recipients	Additional unknown recipients
Content	Generic salutations
	Unexpected timing, type or style of communication from a known sender, such as a friend, co-worker or boss
	Problems with grammar or spelling, including subtle character substitutions, such as 0 (zero) in place of O (the letter O), or 1 (the digit one) in place of l (lower-case letter L)
	Request for highly sensitive information, such as customer account lists, Social Security numbers, credit card numbers, user names or passwords
	Sense of urgency with a request to access links or attachments, provide personal information or initiate a transaction (FINRA observes this frequently in the context of fraudulent wire transfer requests)
	Pressure to bypass or ignore firm policies or procedures
	Notifications that are "too good to be true" (such as winning the lottery or receiving an inheritance)
	Content that is designed to induce an emotional reaction in the recipient, such as political messages, personal attacks or untrue accusations
Attachments and Links	Unexpected attachments, apps or links
	Discrepancy between the written address of the link and its true destination (determined by hovering over the link)
	Suspicious URL patterns where the name of the intended web site appears anywhere other than at the very beginning of the URL
	Upon visiting the site, a message that indicates a problem with the "certificate"

Phishing is a serious threat to firms and their customers. Victims of phishing attacks may release customer, firm, or personal information to cyber criminals; engage in unauthorized wire transfers or payments; or introduce viruses, malware, ransomware, or crimeware that destroys, shuts down, takes over or infects firm systems. Although most firms are aware of the risks posed by phishing attacks, many firms could do much more to strengthen their controls to mitigate this threat.

FINRA has observed firms implementing the following effective practices:

- Creating policies and procedures to specifically address phishing, including but not limited to identifying phishing emails; clarifying that users should not click on any links or open any attachments in phishing emails; requiring deletion of the phishing email; developing a process to securely notify IT administrators and compliance staff; confirming all requests for wire transfers with the customer via telephone or in person;[4] and ensuring proper resolution and remediation after a phishing attack.
- Including phishing scenarios in the firm-level risk assessment process;
- Establishing confirmation policies and procedures for transaction requests over a reasonable threshold (*e.g.*, for a customer money transfer to a new bank or CEO- or CFO-initiated vendor payment) to reduce the likelihood of successful spear phishing or whaling attacks;
- Implementing email scanning and filtering to monitor and block phishing and spam communication;
- Regularly training employees on phishing and related firm policies and procedures (especially for those employees in IT, Human Resources, or customer-facing functions who are more likely to be targeted because of their access to valuable personal and financial information);
- Conducting regular simulated phishing email campaigns to evaluate employee understanding and compliance with the firm's policies and procedures;
- Developing remedial training and imposing appropriate consequences for employees who repeatedly violate the firm's phishing standards or do not demonstrate sufficient sensitivity to phishing risks during the firm's simulated phishing email campaigns;
- Reviewing the firm's processes and procedures to detect and remediate a successful phishing campaign;
- Reducing the impact of a successful phishing attack by segmenting customer and other critical assets, implementing multi-factor authentication and other data loss prevention controls (*see* Data Loss Prevention (DLP) subsection of the Insider Threats section of this report below);
- Maintaining a log of phishing incidents and the firm's responses;
- Establishing a relationship with the local Federal Bureau of Investigation (FBI) office to know when and how to report cyber incidents – including but not limited to phishing attacks – to that office; and
- Reporting such attacks to cybersecurity information-sharing organizations in which they participate.[5]

Since some phishing attacks may begin with successful attacks on customers, firms may wish to direct customers to resources that may help them protect themselves from attack, for example, FINRA's *Phishing and Other Identity Theft Scams: Don't Take the Bait* (Feb. 29, 2012).

Insider Threats

Insider threats remains a critical cybersecurity risk because an insider typically circumvents many firm controls and may cause material data breaches of sensitive customer and firm data. Whether due to malicious behavior—such as a bad actor who plans to sell customer account data on the dark web—or inadvertent error—such as a registered representative who loses his or her laptop or other storage media with unencrypted customer PII—insiders are in a unique position to cause significant harm to an organization. In response to the 2017 and 2018 FINRA Risk Control Assessment (RCA), the vast majority (95-99 percent) of higher revenue firms and 66 percent of mid-level revenue firms indicated that they address insider threats in their cybersecurity programs.

"Insiders" include individuals who currently have or previously had authorized access to firm systems and data because of their function or role and include individuals such as full and part-time employees, contract or temporary employees, consultants and interns, but they may also include employees or contractors of third-party vendors and sub-contractors.

FINRA has observed that effective insider threat programs typically integrate the following components into an overarching, risk-based insider threat program:

- Executive leadership and management support;
- Identity and access management policy and technical controls, including heightened controls, for individuals with privileged access;
- Technical controls including security information and event management (SIEM) and data loss prevention (DLP) tools, as appropriate for the scale and technological sophistication of the firm;
- Training for all insiders; and
- Measures to identify potentially abnormal user behavior in the firm's network.

A comprehensive asset inventory is also a key element of an effective insider threat program (as well as a firm's broader cybersecurity program) and we discuss this in more detail in the branch section of this report as well as FINRA's *Report on Cybersecurity Practices*.

Executive Leadership and Management Support

FINRA has observed the following effective practices by senior executives and management:

- Demonstrating commitment to the firm's cybersecurity policy by personal compliance with its requirements;
- Designating a senior executive or manager with responsibility for the firm's insider threat controls;
- Imposing consequences for all employees violating the policy, regardless of their position or status in the organization;
- Providing timely notifications when access or privileges are changed or an employee resigns, moves to another department or is terminated; and
- Identifying behaviors of potentially malicious insiders and creating a process by which mid-level managers can address such concerns, including escalating the issue to senior leadership, adjusting or eliminating employee privileges or terminating the employee (*see* Identifying Potentially Malicious Insiders section of this report below).

Identity Access Management and User Entitlements

Effective Identity Access Management (IAM) and user entitlements processes can serve as a first line of defense to ensure that all insider users (including contractors, consultants, interns and vendors) are assigned proper access to systems, applications, files and databases. "Proper access" requires that systems entitlements are aligned with specific job functions and assigned only on a need-to-know basis. IAM needs to cover the full lifecycle of entitlements: user on-boarding (*e.g.*, assignment to specific functions and customer accounts), transfers and promotions to new departments/functions and timely off-boarding for users leaving an organization. IAM should also support proper segregation of functions between front office and back office users (*e.g.*, individuals assigned to a trading desk should not have access to wire funds or transfer assets, while individuals assigned to perform reconciliations should not have access to update trading systems).

FINRA has observed firms implementing the following effective practices:

- Establishing and maintaining WSPs to manage the system user access lifecycle (including employee onboarding, departmental and function transfers, promotions and timely terminations of employees, contractors and vendors) where firms typically approve access according to defined procedures and use an auditable ticketing system to document those decisions;
- Conducting periodic review and certification of user entitlements (*e.g.*, annually for all employees, and semi-annually or quarterly for individuals with access to particularly sensitive information or systems or with elevated privileges) and implementing appropriate segregation of duties;
- Implementing comprehensive password policies and controls that require complex passwords, periodic password changes after a specified period of time (and old passwords cannot be re-used) and password locks after a certain number of unsuccessful login attempts;
- Disabling or changing the use of generic IDs (such as vendor-provided "default user" and "administrator" IDs and passwords used for the first time system install) to require individual IDs for each user and strong passwords; and
- Implementing policies and processes to automatically and rapidly revoke network and system access (for example, some firms establish an automated data feed from their human resource system to their identity access management system to drive the creation and removal of basic accounts (such as active directory and email accounts) based on roles).

Privileged User Controls

Privileged users represent a potentially heightened insider threat. Typically, these users are server, network and database administrators who have access to powerful system commands and utilities that enable them to copy, delete or change any data files or system options and parameters (*e.g.*, creating new users with broad system access or elevating other users' or systems' access to firm information). These users may also be able to shut down business applications, networks and processes. In addition, individuals involved in the development, testing, deployment and maintenance of software may possess elevated system privileges. For example, developers may need to be able install software and drivers on their workstations as part of their job function. While these individuals support a firm's information technology infrastructure, their status requires firms to establish appropriate controls to ensure that they have only those privileges necessary for their job function and do not abuse their privileges.

FINRA has observed firms implementing the following effective practices:

- Establishing WSPs to require the monitoring of privileged user system access activities;
- Establishing consistent structures and processes for identifying privileged users;
- Assigning privileged users to special administrative groups and reviewing their activities to identify situations where they may engage in unapproved activities;
- Segmenting privileged users' access according to their roles, including but not limited to development, deployment and maintenance, as well as the change management process;
- Employing a password "vault" to check out one-time passwords in order to enter into an administrative session to protect against password "leakage";
- Using SIEM and other tools to collect and monitor privileged users' activity logs (discussed further below); and
- Requiring multifactor authentication for privileged user logins at all times.

Security Information and Event Management (SIEM) and User and Entity Behavioral Analytic (UEBA) Tools

SIEM tools collect and aggregate and correlate log information from numerous sources, including but not limited to: firewalls, Intrusion Detection and Prevention systems, servers, and network devices. Firms use the aggregated log to monitor various user activities and events. A SIEM system may identify and generate alerts regarding risky activities and potential attacks so that the firm can respond to and prevent sensitive information from going outside the firm's network. In some advanced cybersecurity programs, firms use machine learning in conjunction with SIEM tools to learn and model baseline and irregular behavior, which improves the system's ability to identify potentially malicious behavior, including risky insider activities.

UEBA tools can also enhance a firm's capability to detect anomalous behaviors. Such tools focus on analyzing individual user and entity behaviors, and typically include a learning element that enables the tool, over time, to identify normal and abnormal behaviors and to flag the latter for further review.

FINRA has observed firms implementing the following effective practices:

- Establishing WSPs to require capturing of system logs[6] from sources for aggregation into a SIEM tool;
- Establishing risk-based approaches to identify high risk events, provide timely alerts and escalate events according to agreed procedures;
- Establishing procedures for timely notification when log sources stop sending data to a SIEM tool;
- Implementing behavioral analytics and other artificial intelligence systems to identify emerging trends and suspicious activities in a timely manner;
- Establishing formal change management procedures for SIEM-related rules changes; and
- Maintaining SIEM logs in order to perform historical analysis and forensics.

Data Loss Prevention (DLP)

A strong DLP program creates preventative controls that can help to detect and mitigate insider (and other) threats. DLP controls can prevent the inadvertent or malicious transmission of sensitive customer or firm information to unauthorized recipients. DLP controls typically identify sensitive customer and firm data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method. Whereas some firms maintain DLP software internally, others use vendors to support these efforts.

FINRA has observed firms implementing the following effective practices:

- Establishing a formal DLP program and applicable WSPs to monitor and prevent data breaches;
- Requiring user verification prior to permitting the sending of outbound emails;
- Establishing consistent structures and processes for capturing DLP events—such as outbound emails and attachments or file transfers containing sensitive information—and placing them into quarantine status for compliance review prior to release;
- Establishing robust DLP rules to identify and block or encrypt the transfer of data, such as customer account numbers, Social Security numbers, trade blotter information and source code (and alerting compliance via notification alerts if such rules are violated);
- Establishing rules to control printing of sensitive data and documents;
- Restricting data downloads to USB, CD drives, and SD ports and other mobile devices, as well as blocking access to personal web email programs, cloud-based file sharing service providers and social media sites;
- Implementing robust controls for employees and contractors working from home using personal computers, for example by requiring individuals to use multi-factor authentication and a secure Virtual Private Network (VPN)[7] channel for login, as well as blocking the printing, copying, pasting or saving of firm data to personally owned computers, smartphones or tablets; and
- Installing call verification systems that can potentially screen and identify incoming customer calls to ensure the numbers do not belong to known fraudsters.

Training

As noted, many of the data breaches FINRA has observed occurred because well-intentioned employees or other users made preventable mistakes. Developing a firm culture that focuses on cybersecurity awareness and providing regular cybersecurity training can help address this problem. Effective practices FINRA has observed include firms providing ongoing—rather than one-time—training for staff on:

- Appropriate handling of customers' requests for user name and password changes, money transfers and identity verification, particularly those involving large amounts of money transferred to an overseas location or third parties;
- Sound practices regarding the opening of email attachments and links, including using simulated phishing campaigns where the firm notes and re-tests the individuals who failed the exercise; and
- Identifying social engineering activities from hackers.

A number of firms observed that using actual cases experienced by the firm or peer firms can make the training more interesting and effective for participants.

Identifying Potentially Malicious Insiders

Malicious insider threats are particularly challenging for firms to address. Firms may be over-confident that their hiring practices will ensure "only good people are hired" and that management can identify disgruntled employees through day-to-day interaction. Moreover, malicious insiders know their organization and its weaknesses and can try to work around a firm's controls. Effective programs to identify malicious insiders typically combine people-, process- and technology-based controls. In particular, firms may monitor for non-technical behavior indicators, including but not limited to the following:

Employment Status	Work Patterns	Personality and Personal Circumstances	Unlawful Activities
Received warning, otherwise not in "good standing" or under review for termination of employment	Change of working pattern	Drastic change in personality or behavior	Notification or evidence of criminal activity
Concerns about missed promotions	Unexcused or unauthorized absences	Threats of retaliation	Acts or threats of violence
Notification or discussion regarding leaving the company	Decline in performance	Harassment	Destruction of property
Searching for new jobs	Conflicts at work	Significant debt and recurring financial irresponsibility	Attempts to bypass/ defeat any security system
			Time and attendance fraud
			Falsifying reports or records
			Theft

In addition to implementing the policy and technical measures described in the sections above, FINRA has observed firms that implement the following effective practices:

- Cultivating a strong culture of compliance that encourages confidential reporting of potentially suspicious activity (*e.g.*, "if you see something, say something"); and
- Performing regular reviews of individuals with higher risk combinations of privileges, especially in environments where it is difficult to maintain segregation of duties.

Penetration Testing

Penetration testing (or a pen test) is an important element in many firms' cybersecurity programs. A pen test simulates an attack on a firm's internally- or externally-facing computer network to determine the degree to which malicious actors may be able to exploit vulnerabilities in the network and evaluate the effectiveness of the firm's protective measures.[8] For example, one particular type of pen test focuses on a firm's web application to evaluate its security design and associated databases (*e.g.*, a firm's public website where employees, representatives or customers log in to access account and position data, including PII or other confidential information).[9] The pen test process requires an active analysis of a firms' network, applications or other targets for any weaknesses, technical flaws, gaps or vulnerabilities. Such testing often involves both automated scanning tools and manual techniques and may include social engineering. Any identified security issues would be presented to the business owner and information technology management, together with an assessment of the impact, risk classification of findings, and a proposal for mitigation or a technical solution.

Pen tests may take the perspective of an outside attacker attempting to infiltrate a firm's system or an insider attacker trying to gain access to assets to which they should not have access. Both types of tests can be performed in different modes: (1) "White Box" mode where the test team knows something about the system such as a range of IP addresses, software packages in use or a user ID; (2) "Black Box" mode in which the test team knows nothing about the system; or (3) "Gray Box" mode where the test team has some limited information about the system.

According to FINRA's 2018 RCA, 100 percent of higher revenue firms include penetration testing as a component in their overall cybersecurity program. The utility of pen tests is less a function of firm size, however, and much more a function of a firm's business model and technology infrastructure. For example, pen tests are highly relevant to firms that provide online access to customer accounts. FINRA has observed higher, mid-level and lower revenue firms that conduct pen tests. Other factors these firms consider in evaluating the relevance of penetration testing include the degree to which they manage or store confidential or critical data such as trading strategies, customer PII, information about mergers and acquisitions or confidential information from other entities (for example, in the case of clearing firms).

FINRA has observed firms implementing the following effective practices:

- Adopting a risk-based approach to penetration testing;
- Thoroughly vetting their testing providers;
- Establishing contractual provisions that carefully prescribe vendor responsibilities;
- Rigorously managing and responding pen test results; and
- Periodically rotating testing providers to benefit from a range of skills and expertise.

Risk-Based Approach

Many firms determined the systems to be tested and the frequency with which they should be tested based on a risk assessment where higher risk systems were tested more frequently. Factors firms considered in identifying high risk systems included the sensitivity of the data contained or accessed by that system, the operational importance of the system and the presence of any known vulnerabilities.

Also, firms with strong cybersecurity programs conducted pen tests at least annually and more frequently for mission critical, high risk systems such as for an online trading system. In addition to a calendar-based approach to testing, some also perform risk-based penetration tests after key events, such as any time a significant change is made to important elements of the firm's applications and systems infrastructure.

Vendor Selection and Due Diligence

Firms generally used third parties to perform pen tests (even for those tests that take an "insider" view). Firms conducted thorough due diligence to select vendors with a sound knowledge of cyber risks, current attack techniques and appropriate tools to emulate the actions of an attacker. Moreover, some firms required vendors to provide an ethical hacking certification such as Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP) or GIAC Penetration Tester (GPEN) certifications prior to an engagement. Firms may alternate between providers, or use multiple providers, to maximize the likelihood of identifying issues. In some cases, firms with sufficient resources to develop this specialized skill set conducted pen tests using their own staff.

Contractual Arrangements

Firms typically established a written contract with the vendor performing the pen test. That contract specified what the vendor should and should not do during the test, for example, which applications, systems, networks or IP addresses the vendor should test; the degree to which the vendor should attempt to exploit a system if a control is breached (*e.g.*, a firewall or user entitlements); or the time of day the pen test should take place (*e.g.*, to avoid an simulated attack during peak usage period). Contracts also typically specified vendor responsibility for non-disclosure of confidential information or findings, as well as the details the vendor would report to the firm. Pen tests took place on both an announced and unannounced basis, although in the latter case, at least some firm staff were aware of the planned timing for the test.

Pen Test Results

Firms established governance structures and procedures to assess the risk level and determine how quickly the firm would mitigate issues identified during the pen tests. Typically firms, or the pen test vendor, assigned a risk level (*e.g.*, critical, high, medium, low); systematically tracked issues identified along with their risk level; and addressed the higher risk levels more quickly. This process was completed in accordance with prescribed policies that included escalation requirements for particularly serious risks and documentation requirements regarding the measures implemented to mitigate the vulnerability. In some cases, firms conducted a follow-up pen test to assess the effectiveness of mitigation measures adopted to address a previously identified control weakness.

Mobile Devices

The widespread and expanding use of mobile devices creates new opportunities for attacks on sensitive customer and firm data. Employees, customers, consultants and contractors may regularly use smartphones, tablets, laptops and other devices for a variety of activities, including communication, trading, receiving investment alerts, money transfers and account monitoring.[10] As the industry becomes more reliant on mobile devices, risks associated with this technology continue to increase. Firm and personal mobile devices are exposed to risks including, but not limited to, malicious advertisements and spam communication; infected, cloned or pirated mobile applications; vulnerabilities in mobile operating systems; and phishing, spoofing or rerouting of calls, emails and text messages (*see* Phishing section of this report above). Although all firms offering access to their systems through mobile devices face such risks, firms with large numbers of retail customers may be subject to greater exposure and should consider especially rigorous implementation of cybersecurity controls to protect firm and customer information.

FINRA has observed firms implementing the following effective practices for their employees, consultants and contractors:

- Developing policies and procedures addressing employee obligations to protect customer and firm information and "bring your own device" standards for the use of personal devices for firm business;[11]
- Prohibiting the use of personal devices for firm business (including email, texting, messaging or any other communication) unless the devices have been approved by the firm, and the employee has signed an attestation agreeing to comply with the firm's policies and procedures;
- Including reviews of mobile device security controls in branch office audits and inspections, including for remote employees and branch office staff (*see* Data Loss Prevention and Branch Controls sections of this report above);
- Ensuring that firm compliance and technology support staff have sufficient expertise in mobile cybersecurity issues;
- Providing regular training to all firm employees, consultants and contractors on firm mobile device requirements and effective practices to protect mobile devices;
- Maintaining an inventory of all personal and firm devices used to access firm systems and data;
- Requiring all personal devices to maintain a separate, secure, encrypted mobile device management (MDM) application for all firm activities, including email communication, calendar and other activities;
- Enforcing the use of passwords and setting password standards for length and complexity;
- Setting time-outs after certain periods of non-usage;
- Installing security software and antivirus software to protect all mobile devices used to engage in firm business and monitor for compliance with firm security standards;
- Implementing authorization and authentication controls in "offline" mode;
- Removing all software, services and applications that violate the firm's security policy;
- Implementing transmission controls for secure transfer of data between the mobile device and the firm's servers;
- Emphasizing the importance of physically securing all personal and firm devices at all times to prevent the risk of theft or loss;
- Implementing reporting procedures for lost personal or firm devices;
- Maintaining an inventory of all lost personal and firm devices, including the type of remediation taken to reduce or eliminate the risk of exposure of firm or customer information;
- Ensuring that the firm is able to remotely wipe firm data from a device that belongs to a former employee or from a device that an employee has lost; and
- Enforcing mobile device policies and procedures by pursuing consequences for violations, including but not limited to additional training, written notices, fines, suspension, or termination of employment.

FINRA has also observed firms implementing the following effective practices for their customers:

- Monitoring mobile application markets on the dark web for malicious applications that impersonate the firm's mobile application;
- Informing customers about the risks of accessing and storing personal and financial data on their mobile devices;
- Advising customers about the risks of "jailbreaking" or "rooting" mobile devices to make them "open" for unauthorized applications, games and networking tools, which increase the risks of viruses, malicious code and unauthorized modifications to operating systems;
- Requiring multi-factor authentication for access to customer accounts and trading applications and other data loss prevention controls (*see* Data Loss Prevention (DLP) subsection of the Insider Threats section of this report above);
- Restricting certain changes to account settings, financial information or contact information via mobile device and requiring customers to contact their advisor for such requests;
- Maintaining account and trading session security by automatically terminating access after a certain period of inactivity; and
- Ensuring secure development and testing procedures when releasing or changing mobile account or trading applications (*e.g.*, scanning for security vulnerabilities and performing pen tests for mobile platforms prior to release).

Appendix: Core Cybersecurity Controls for Small Firms

The following list identifies core controls that are likely to be relevant to many small firms' cybersecurity programs. To establish an effective program, however, firms will need to consider these measures in the context of their business model and technology infrastructure, along with other factors that should inform firms' cybersecurity programs. In addition to this report, FINRA has provided a number of cybersecurity *resources* for small firms, such as the 2015 FINRA *Report on Cybersecurity Practices* ("the 2015 Report") and FINRA's *Small Firm Cybersecurity Checklist* ("the Checklist"). Use of this list does not create a "safe harbor" with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements.

- **Patch Maintenance.** Enable the automatic patching and updating features of operating systems and other software to help firms maintain the latest security controls (*see* Sections 4 and 5 of the Checklist).
- **Secure System Configuration.** When configuring systems and software, use vendor guidance or industry standards, such as those published by the Center for Internet Security ("CIS") (*see* Overview and Resources section of the Checklist).
- **Identity and Access Management.** Limit access to confidential customer and firm information based on business need. Tightly restrict use of "admin" or highly privileged entitlements and regularly review user accounts and privileges to modify or delete those which are no longer necessary to achieve business objectives (*see* the Insider Threats section of this report, Technical Controls section of the 2015 Report and Section 8 of the Checklist).
- **Vulnerability Scanning.** Use Commercial Off-The-Shelf ("COTS") software or third-party vendors to continuously scan for vulnerabilities and quickly address detected discrepancies (*see* the Phishing section of this report, the Cybersecurity Risk Assessment as well as Technical Controls sections of the 2015 Report and Section 10 of the Checklist).
- **Endpoint Malware Protection.** Install COTS software on firm computers, servers and firewalls to detect and block viruses and other malware (*see* the Technical Controls section of the 2015 Report and Sections 4 and 5 of the Checklist).
- **E-mail and Browser Protection.** Install software or use services to block web-based e-mail programs and unsafe content received through e-mail (*e.g.*, phishing attacks) or accessed via web browsers (*see* the Phishing section of this report and Sections 4 and 5 of the Checklist).
- **Perimeter Security.** Use network access controls, such as firewalls, to block unnecessary connectivity between firm systems and outside systems. If feasible, incorporate an Intrusion Detection and Prevention capability (*see* the Insider Threats section of this report, Technical Controls section of the 2015 Report and Sections 4, 5 and 10 of the Checklist).
- **Security Awareness Training.** Provide cybersecurity training to all employees upon their employment and at least annually thereafter (but preferably more often) to ensure all users are aware of their responsibilities for protecting the firm's systems and information. Training should address common attacks, how to avoid becoming a victim and what to do if you notice something suspicious. Consider implementing an ongoing phishing awareness campaign (*see* the Insider Threats section of this report, Staff Training section of the 2015 Report and Section 8 of the Checklist).
- **Risk Assessments.** Conduct annual risk assessments and testing of firm controls to verify effectiveness and adequacy. This assessment may be accomplished using third-party or firm security experts (*see* Cybersecurity Risk Assessment section of the 2015 Report and Sections 1 and 2 of the Checklist).

- **Data Protection.** Encrypt critical data, back it up frequently and store copies of back-ups offline. Regularly test the firm's ability to restore data. Consider blocking USB ports and use of all removable data storage devices, including CDs and flash drives (*see* Sections 4, 5, 6 and 12 of the Checklist).
- **Third-Party Risk Management.** Review System and Organization Controls (SOC) or SSAE 18 reports for third party vendors and other partners with access to confidential firm and customer data to ensure they have security controls commensurate with, or better, than the firm's. All contracts should have provisions to enforce controls to protect data, including prompt notification of any changes to those controls and vulnerabilities or breaches that may affect the firm (*see* the Vendor Management section of the 2015 Report and Section 3 of the Checklist).
- **Branch Controls.** Ensure that branches apply and enforce relevant firm cybersecurity controls, which may include many of the controls identified in this list, as well as other relevant controls such as those elsewhere in this report or in the Small Firm Cybersecurity Checklist (*see* the Branch Controls section of this report).
- **Policies and Procedures.** Create policies and procedures that address each category of controls applicable to the firm, such as those identified in this list (*see* the Governance and Risk Management for Cybersecurity section of the 2015 Report).

Endnotes

1. On an annual basis for the past seven years, FINRA has conducted a voluntary Risk Control Assessment (RCA) Survey with all active member firms. The RCA segments firms based on their business activities and other characteristics, including, but not limited to, their revenue. In order to share some of the insights from the RCA, we provide the relevant data for firms with higher revenue, firms with mid-level revenue and firms with lower levels of revenue. The 2018 RCA shows that 95 percent of higher revenue firms maintain a branch password policy; 90 percent maintain a process for the installation of system patches across branches; 85 percent require encryption of hard drives; 79 percent implement an electronic communication usage policy; 78 percent require up-to-date virus protection; and 75 percent have network security standards.

2. According to the 2018 RCA, 60 percent of higher revenue firms maintain branch-level registered representative training requirements.

3. According to the 2018 RCA, 94 percent of higher revenue firms and 70 percent of mid-level revenue firms use a risk assessment as part of their cybersecurity program.

4. *See FINRA Regulatory Notice 09-64* for additional information on verifying instructions to transmit or withdraw assets from customer accounts.

5. One example of such an organization is the Financial Services – Information Sharing and Analysis Center (FS-ISAC).

6. "System logs" refers to data stored that creates an audit trail of events that occur on, and tasks performed by, a computer's hardware and software.

7. A VPN provides a secure, encrypted communications channel between a remote user over a public network, typically the internet, and a company's secure network.

8. Pen tests are distinct from "vulnerability assessments." The latter are typically performed on a routine basis, in some cases daily, using automated tools – such as web and network scanners – and look across multiple firm systems. An example of vulnerability scanning may include checking servers for security patches to ensure they are current.

9. In response to FINRA's 2016 and 2018 RCAs, 89 percent of higher revenue firms, 71 percent of mid-level revenue firms and 47 percent of lower revenue firms reported that they manage or store confidential customer information. Accordingly, all firms should recognize their need to monitor and safeguard confidential customer data.

10. According to the 2018 RCA, 55 percent of higher revenue firms and 28 percent of mid-level revenue firms provide retail customers access to their accounts via a website browser on a mobile device and 35 percent of higher revenue firms and 14 percent of mid-level revenue firms provide such access via mobile apps.

11. According to the 2018 RCA, 93 percent of higher revenue firms maintain a firm-wide mobile device policy and 29 percent maintain a branch-specific mobile device policy.

Investor protection. Market integrity.

1735 K Street, NW
Washington, DC 20006-1506

www.finra.org

18_0299.1 –12/18

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

LINDABETH RIVERA and JOSEPH WEISS, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	No. 16 C 02714
v.	)	
	)	Judge Edmond E. Chang
GOOGLE, INC.,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Under the Illinois Biometric Privacy Act, a private entity cannot collect or store certain kinds of biometric information, including face-geometry scans, without first obtaining consent or providing certain disclosures. 740 ILCS 14/1 *et seq*. Plaintiffs Lindabeth Rivera and Joseph Weiss both allege that Google unlawfully collected, stored, and exploited their face-geometry scans via Google Photos, a cloud-based service.[1] R. 63, Second Am. Compl. ¶¶ 4-5, 28-30, 33-36, 38-39, 42-45, 57-60, 67-70;

[1]The Court has diversity jurisdiction over Rivera's and Weiss's state-law claims under 28 U.S.C. § 1332. Rivera and Weiss are citizens of Illinois. R. 63, Second Am. Compl. ¶¶ 7-8. Google is a citizen of Delaware (its place of incorporation) and California (its principal place of business). *Id.* ¶ 9. Although Google, Inc. has since reorganized from a corporation to a limited liability company, FCC Report. No. SCL-00205 (Nov. 24, 2017), "the jurisdiction of the court depends upon the state of things at the time of the action brought," *Grupo Dataflux v. Atlas Glob. Grp., L.P.*, 541 U.S. 567, 570 (2004) (quotation omitted).

The amount in controversy requirement is also satisfied. The aggregate claims of the potential class (which would number in the thousands of members) could possibly equal or exceed $5,000,000, exclusive of interest and costs. 28 U.S.C. § 1332(d)(6). Even setting aside the class allegation, it is not "legally impossible" for either Weiss or Rivera alone to recover more than $75,000 in this action. *Back Doctors Ltd. v. Metro. Prop. & Cas. Ins. Co.*, 637 F.3d

see also R. 167, Pl.'s Resp. Br. at 1-3.[2] Google now moves for summary judgment on all of Plaintiffs' claims against it, arguing that Plaintiffs cannot establish Article III standing; Plaintiffs are not "aggrieved" within the meaning of the Act; and Plaintiffs are not entitled to monetary or injunctive relief under the Act because they have suffered no harm.[3] R. 151, Def.'s Mot. Summ. J.

For the reasons discussed below, Plaintiffs have not suffered an injury sufficient to establish Article III standing and their claims are dismissed. Because the Court lacks subject matter jurisdiction over Plaintiffs' claims, the Court need not consider Google's other arguments.

I. Background

In deciding Google's motion for summary judgment, the Court views the evidence in the light most favorable to Plaintiffs, the non-moving parties. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986). Google Photos is a free, cloud-based service for organizing and sharing photographs. R. 153, Def. SOF ¶ 7; R. 167-1, Pls. Resp. Def. SOF ¶ 10. When a user uploads a photo to Google Photos, Google Photos detects images of faces, then creates a face template, represented by [redacted]

827, 830 (7th Cir. 2011) (amount-in-controversy requirement satisfied unless it is "legally impossible" for a plaintiff to recover that amount).

[2]Citations to the record are noted as "R." followed by the docket number and the page or paragraph number.

[3]The parties agreed to defer argument on and resolution of other issues, such as liability under the Act (whether face templates qualify as "biometric identifiers" or "biometric information" under the Act, and whether Google provided sufficient disclosures or obtained sufficient consent), Google's defense under the Dormant Commerce Clause, whether the Act applies extraterritorially, and choice of law. R. 137, Joint Status Report 03/28/18; *see also* R. 152, Def.'s Br. at 4 n.2. Where relevant, the Court will note when it is assuming certain facts in favor of Plaintiffs for the purposes of this Opinion, even though Google has not conceded the issue outside of the motion under consideration.

[redacted]. Def. SOF ¶¶ 13-15. Google uses these face templates to compare the visual similarity of faces within Google Photos users' private accounts, *id.* ¶ 15, and then groups photographs with visually similar faces and displays the groups (called "face groups") to the users' private account, *id.* ¶ 9. Google Photos' face-recognition feature automatically defaults to "on" and is applied to every photo uploaded to the service unless the user opts out. Pls. Resp. Def. SOF ¶¶ 8, 10. The technology also can be applied to photos on the user's phone if "Private Face Clustering" is enabled. *Id.* ¶ 10. Google Photos users can assign a label (for example a name or title) to any face groups in their private accounts. Def. SOF ¶ 18. These face labels are private to individual users' accounts and are visible only to that user and to Google.[4] *Id.* ¶ 20. Google does not use the face templates it creates for anything other than organizing photographs in users' Google Photos accounts.[5] *Id.* ¶ 59.

[4]Plaintiffs dispute this, contending that "[l]abels, face templates, and all associated data in Google Photos are accessible to Google, its personnel, and to any party that Google permits to access such data." Pls. Resp. Def. SOF ¶ 20 (citing R. 153-3, Porter Decl. ¶¶ 4-10). But Porter's declaration states that the Plaintiffs' face templates are private to their accounts, and that the labeled face group of Rivera has not been "disclosed to anyone outside of Google." Porter Decl. ¶¶ 6-7. And Plaintiffs do not dispute that "[t]here is no evidence that the … face labels from the photographs of [Plaintiffs] … have been shared outside of Google." Pls. Resp. Def. SOF ¶ 52. There is no genuine dispute of material fact that face labels are visible only to the user and Google.

[5]Plaintiffs also dispute this, and argue that "the facial recognition … can be monetized by Google." Pls. Resp. Def. SOF ¶ 59; R. 167-1, Pls. Statement Add. Facts ¶ 6. As discussed in more depth below, the only evidence offered by Plaintiffs shows that Google *might* use this technology to mine data or target advertisements in the *future*. Pls. Resp. Def. SOF ¶ 59; Pls. Statement Add. Facts ¶ 6. Although that sort of use without obtaining the proper consent might very well constitute a concrete injury, Plaintiffs provide no evidence that Google has engaged in those practices with respect to Plaintiffs' face templates or photographs.

Weiss is a Google Photos user, Def. SOF ¶ 24, and the face-grouping feature in his account was defaulted to "on" until he turned it off sometime in mid-December 2017, Pls. Resp. Def. SOF ¶ 25. There are 53 photographs of Weiss that form the basis of his claim. Def. SOF ¶ 26. At least 16 of them were taken after he filed his complaint on March 4, 2016, but before he turned off the face-grouping feature. *Id.* ¶ 27. Weiss's Google Photos account, which is associated with his face template, is also associated with his Gmail account. Pls. Resp. Def. SOF ¶ 53. On the other hand, Rivera is not a Google Photos user, Def. SOF ¶ 31, but her friend Blanca Gutierrez is,[6] *id.* ¶¶ 32-33. The face-grouping feature was defaulted to "on" in Gutierrez's Google Photos account. Pls.' Resp. Def. SOF ¶ 34. There are at least 27 photos of Rivera taken by Gutierrez and uploaded to Gutierrez's Google Photos account that form the basis for Rivera's claim. *Id.* ¶¶ 35-36. At least 10 of the photographs of Rivera uploaded to Gutierrez's Google Photos account were taken after Rivera filed her complaint. Def. SOF ¶ 38. Gutierrez labeled a face group in her account as "LindaBeth Rivera." *Id.* ¶ 44. Apart from Weiss's Gmail account and Gutierrez's labelled face group, Plaintiffs' face templates are not associated with other identifying information, such as their social security numbers or credit card information. Pls. Resp. Def. SOF ¶¶ 53-54. Google did not have permission from Plaintiffs to capture, store, or use face scans of Plaintiffs.[7] Pls. Statement Add. Facts ¶ 2.

---

[6]Ms. Gutierrez is not a party to this action. Def. SOF ¶ 32.

[7]Google disputes whether it obtained consent or provided notice in compliance with the Act, 740 ILCS 14/15. R. 179-1, Def. Resp. Pls. Statement Add. Facts ¶ 2. As noted earlier, resolution of that issue was deferred to after the resolution of this motion. *Id.*; Joint Status Report 03/28/18. For the purposes of this motion, the Court assumes that Google did not obtain sufficient consent.

Weiss and Rivera both claim injury to their privacy interests, but testified that they did not suffer any financial, physical, or emotional injury apart from feeling offended by the unauthorized collection. R. 179-1, Def. Resp. Pls. Statement Add. Facts. ¶¶ 3-4. Weiss testified that he would not have given consent to collect his face template if Google had asked him to do so, although he was not sure if he would have stopped using Google Photos altogether. Pls. Resp. Def. SOF ¶ 29. The face templates and face groups associated with Weiss's and Gutierrez's Google Photos accounts are private, and there is no evidence of any unauthorized access into the accounts. Def. SOF ¶¶ 49-50.

II. Standard

Summary judgment must be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A genuine issue of material fact exists if "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). In evaluating summary judgment motions, courts must view the facts and draw reasonable inferences in the light most favorable to the non-moving party. *Scott v. Harris*, 550 U.S. 372, 378 (2007). The Court may not weigh conflicting evidence or make credibility determinations, *Omnicare, Inc. v. UnitedHealth Grp., Inc.*, 629 F.3d 697, 704 (7th Cir. 2011), and must consider only evidence that can "be presented in a form that would be admissible in evidence." Fed. R. Civ. P. 56(c)(2). The party seeking summary judgment has the initial burden of showing that there is no genuine dispute

and that they are entitled to judgment as a matter of law. *Carmichael v. Village of Palatine*, 605 F.3d 451, 460 (7th Cir. 2010); *see also Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986); *Wheeler v. Lawson*, 539 F.3d 629, 634 (7th Cir. 2008). If this burden is met, the adverse party must then "set forth specific facts showing that there is a genuine issue for trial." *Anderson*, 477 U.S. at 256.

III. Analysis

Google argues that this Court lacks subject matter jurisdiction over this case because Plaintiffs have not shown they have suffered concrete injuries sufficient to satisfy Article III standing, and even if Plaintiffs could establish concrete injuries, those injuries were not caused by Google's conduct. Standing requires that a plaintiff "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citations omitted). Predictably, the parties dispute how the Court should apply the Supreme Court's most recent pronouncement on the injury-in-fact requirement, *Spokeo v. Robins*, so it is worth examining that opinion before delving into the facts of this case.

A. *Spokeo*

A plaintiff can, in some instances, satisfy the concrete-injury requirement of Article III absent actual monetary damages. But in those cases, federal courts must carefully ensure that the concrete-injury requirement is still met. In *Spokeo*, the plaintiff alleged that an online personal-information publisher violated the Fair Credit Reporting Act by publishing inaccurate information about him. 136 S. Ct. at

1546. The website got several things wrong, incorrectly reporting that "he is married, has children, is in his 50's, has a job, is relatively affluent, and holds a graduate degree." *Id.* But despite these mistakes, the plaintiff did not allege that he suffered any actual monetary harm. *Id.* at 1546, 1550. Even without that allegation, the Supreme Court reiterated that the concrete-injury requirement can be satisfied even if the injury is not tangible. *Id.* at 1549. The Court explained, "[a]lthough tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that *intangible* injuries can nevertheless be concrete." *Id.* (emphasis added).[8]

In determining which intangible injuries are sufficient to confer standing and which are not, *Spokeo* set out basic principles: a "bare procedural violation" of a statute is *not* automatically enough to satisfy Article III's concreteness requirement. 136 S. Ct. at 1549. To be sure (and as Plaintiffs here discuss in detail), "[i]n determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles." *Id.* When Congress has created a cause of action for a statutory violation, by definition it has created a legally protected interest that Congress, at least, deems important enough for a lawsuit. Going beyond *federal* statutes, the Seventh Circuit has recognized the importance of state legislative judgments as well. *See Scanlan v. Eisenberg*, 669 F.3d 838, 845 (7th Cir. 2012) (noting the importance of federal congressional judgments and reasoning "the

[8]At the same time, concreteness is indeed a requirement that is separate and apart from the Article III requirement that the injury be "particularized" to the individual plaintiff. *Spokeo*, 136 S. Ct. at 1548. Specifically, "[t]o establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete *and* particularized.'" *Id.* at 1548 (emphasis added) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)).

same must also be true of legal rights growing out of state law") (cleaned up).[9] *Spokeo* explained that the legislative branch, with its fact-finding ability and responsiveness to public interest, "is well positioned to identify intangible harms that meet minimum Article III requirements," so Congress's (or the state legislature's) judgment on the nature of the injury is "instructive and important." 136 S. Ct. at 1549. Still, "Congress' role in identifying and elevating intangible harms does *not* mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right … . Article III standing requires a concrete injury even in the context of a statutory violation." *Id.* (emphasis added).

Spokeo also announced the principle that the *risk* of harm sometimes is enough to satisfy concreteness. 136 S. Ct. at 1549. To illustrate this point, the Supreme Court offered both a historical example and a statute-based example. From history and the common law, *Spokeo* noted that common law defamation cases have long allowed plaintiffs to sue even though their actual damages are difficult to prove. *Id.* From Congress, *Spokeo* cited two information-rights cases, *Federal Election Comm'n v. Akins*, 524 U.S. 11, 20-25 (1998), and *Pub. Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 449 (1989), both of which involved plaintiffs who sought information that Congress had decided to make available to the public. *Spokeo*, 136 S. Ct. at 1549-50. There was no particular *substantive* standard of conduct set by the pertinent provisions of the information-access statutes involved in those cases. Indeed, *Public*

[9]This Opinion uses (cleaned up) to indicate that internal quotation marks, alterations, and citations have been omitted from quotations. *See* Jack Metzler, *Cleaning Up Quotations*, 18 Journal of Appellate Practice and Process 143 (2017).

Citizen cited to prior cases involving the Freedom of Information Act, and declared, "Our decisions interpreting the Freedom of Information Act have never suggested that those requesting information under it need show more than that they sought and were denied specific agency records." *Pub. Citizen*, 491 U.S. at 449 (citing cases). These *procedural*-rights-only cases led *Spokeo* to explain that "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress identified." 136 S. Ct. at 1549 (emphasis in original).

Applying these principles to this case, with the aid of more recent Seventh Circuit cases, it is clear that Google's retention of Plaintiffs' unique face templates did not cause them a concrete injury for Article III standing purposes. The more difficult question is whether the creation of the face templates constitutes an injury-in-fact on its own. But that too falls short of satisfying Article III's concreteness requirement.

B. Retention of Face Scans

First up is Plaintiffs' claim that Google retained or stored their face templates in violation of the Act.[10] The Act requires that any private entity in possession of biometric information or identifiers must develop and make available to the public a retention schedule and guidelines for destroying that information, 740 ILCS 14/15(a),

[10]As noted earlier, for the purposes of deciding this motion, the Court assumes that the face templates are "biometric identifiers" under the Act, 740 ILCS 14/10, and that Google did not provide disclosures or obtain the consent as required by the Act, *id.* § 14/15.

and provides certain standards for storing, transmitting, and protecting the information, *id.* § 14/15(e). By not providing the required disclosure or obtaining the required consent, Plaintiffs argue that Google violated their right to control their own biometric identifiers and information, which Plaintiffs assert is a right of privacy. Pls.' Resp. Br. at 3-4 (citing Pls. Statement Add. Facts ¶ 3 (quoting Weiss Dep. Tr. at 176:21-177:2 ("I believe that my biometric information or identifier is very sensitive. I think it's akin to my DNA, to a fingerprint. To have that stored, collected, is, again, that in and of itself, when done so against my consent or without my consent, it's a damage, I think.")); Pls. Statement Add. Facts ¶ 4 (citing Rivera Dep Tr. at 78:10-14)); R. 166-2, Exh. B, Rivera Dep Tr. at 59:15-19 ("Google is putting me at risk for potential hackers. … I feel like it's putting me—pretty much my identity in danger."); *id.* at 61:8-9 ("I feel like my identity was harmed so that is my property.").

The Seventh Circuit has definitively held that retention of an individual's private information, on its own, is not a concrete injury sufficient to satisfy Article III. *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912-13 (7th Cir. 2016). In *Gubala*, a cable subscriber alleged that Time Warner Cable had unlawfully retained information that he had provided—including his date of birth, address, phone number, and social security number—in violation of the Cable Communications Policy Act. *Id.* at 910. The Seventh Circuit acknowledged that there would be "a *risk* of harm" if Time Warner had "given away or leaked or lost any of his personal information or ... ha[d] the information stolen from it." *Id.* (emphasis in original). But there were no facts suggesting that the information had been further disclosed or that

there truly was a risk of disclosure. *Id.* at 910-11. So even though the statute was violated, *Gubala* held that mere retention of an individual's personal data (without disclosure or risk of disclosure) was insufficient to confer Article III standing. *Id.* at 912-13. Yes, the subscriber did "*feel* aggrieved," but that by itself did not cause him a concrete injury. *Id.* at 911 (emphasis in original); *see also Groshek v. Time Warner Cable, Inc.*, 865 F.3d 884, 886-87, 889 (7th Cir. 2017) (plaintiff lacked standing to sue for a violation of the Fair Credit Reporting Act where the defendant obtained a credit report without providing the required disclosures; although the defendant's action violated plaintiff's privacy, it was merely a "statutory violation completely removed from any concrete harm or appreciable risk of harm").

Setting aside *how* Google obtained Plaintiffs' face templates (which will be addressed in the following section), Plaintiffs have not offered evidence about the retention of their face templates that overcomes the obstacle in *Gubala.* Plaintiffs do not dispute that: their face templates have not been shared with other Google Photos users or with anyone outside of Google itself; there has not been any unauthorized access to the accounts or data associated with their face templates or face groups; and hackers have not obtained their data. Pls. Resp. Def. SOF ¶¶ 49-52. In other words, all that Plaintiffs can point to on the issue of retention is a privacy concern that *Gubala* holds is insufficient to satisfy Article III's concrete-injury requirement.

To demonstrate a heightened risk of harm, Plaintiffs filed a notice of supplemental information, with an accompanying news article and a Google blog entry, reporting that a software bug gave outside developers access to the data of

around 500,000 Google+ users between 2015 and March 2018. R. 203, Exh. A, 10/08/18 WSJ Article; *id.*, Exh. B, 10/08/18 Project Strobe Blog. Google+ is another Google product, distinct from Google Photos. According to Plaintiffs, the exhibits show that Google decided not to disclose the issue to avoid regulatory scrutiny and reputational damage. *Id.* More recently, Plaintiffs filed another notice, which reports yet another software bug that compromised the private information of around 52½ million Google+ users, which Google again kept quiet for about a week before disclosing. R. 204, Exh. A, 12/10/18 The Keyword Blog. Even assuming, as is appropriate at summary judgment, that these breaches happened and that Google failed to disclose them fast enough, these disclosures have little bearing on the facts of *this* case. None of the disclosures pertain to the accounts of Google Photos users, nor is there any evidence of a connection between the disclosures of Google+ account data to Google Photos accounts or data. *Id.* So this newly presented information does not create a genuine dispute undermining Google's argument that "[t]here is no evidence of any unauthorized access to the *Google Photos accounts* and related data of Weiss and Gutierrez," Def. SOF ¶ 50 (emphasis added), nor is there "evidence that the face templates, face groups, or face labels from the photographs of Weiss and Rivera in Weiss and Gutierrez's *Google Photos accounts*, respectively, have been shared outside of Google." *Id.* ¶ 52 (emphasis added).[11]

[11]Although neither party discusses Google Photo Application Programming Interfaces (APIs), it appears that there are APIs for Google Photos. *See* R. 166-2, Maya Decl., Exh. H (email from Google employee thanking a person from "PM Mobile Vision APIs/Platform" for help with improving FaceNet technology); *see also* https://developers.google.com/photos/ (website for Google Photos APIs). "Google makes user data available to outside developers through more than 130 different public channels known as application programming

When a plaintiff relies on a risk of future harm to satisfy Article III's injury requirement, the plaintiff must establish, at the very least, a "substantial risk" that the future harm will occur. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013). The circumstances underlying the Google+ data breach do not come close to the kinds of situations in which the risk of future harm satisfies Article III concreteness requirements. *Compare Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968-69 (7th Cir. 2016) (hackers already had breached the defendant's database and stolen customers' payment-card information, so the risk of identity theft and the precautions customers took to mitigate the risk constituted a concrete injury) and *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (same), *with In re VTech Data Breach Litig.*, 2017 WL 2880102, at *4-5 (N.D. Ill. July 5, 2017) (a hacker accessed and copied plaintiffs' data—including names, addresses, and birthdates—from defendant's online communication platform connected to a children's game, but because plaintiffs did not plausibly allege that the disclosure of that data increased their risk of identity theft or fraudulent transactions, they lacked standing). It is true that the Illinois legislature has concluded that identity theft of

---

interfaces, or APIs." 10/08/18 WSJ Article at 2. But the mere existence of APIs does not mean that, without a bug, Google was sharing photos or face templates with outside parties, since APIs "usually require a user's permission to access any information … ." *Id.* So Plaintiffs could not rely on the mere existence of Google Photo APIs to confer standing (nor have they done so in any filing).

The Google+ bugs affected Google+ APIs, so ostensibly a bug causing a data breach *could* also affect a Google Photos API. But as noted above, there is no evidence that any such bug has affected Google Photos or any Google Photos APIs, so any such harm is purely speculative. That said, if Google is aware of any bug or data breach to any Google Photos API or Google Photos itself, it should have already reported them to Plaintiffs (as supplemental discovery) and to the Court (in a supplemental filing), and must do so immediately if a Google Photos breach occurred.

biometric information poses an additional harm beyond theft of other personal identifiers: it is not as easy to change biometric information as it is to get a new social security number or a new credit card number, *see* 740 ILCS 14/5(c) ("Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information … once compromised, the individual has no recourse … ."). But Plaintiffs here have not offered enough evidence, even when viewed in their favor, demonstrating a substantial risk that their own information will be disseminated to anyone outside of Google. The Google+ data breach does not support Article III standing.

With regard to the retention violation, all Plaintiffs are left with is their testimony that they felt their privacy rights were violated, but "*feel*[*ing*] aggrieved," without more, does not establish a concrete injury. *Gubala*, 846 F.3d at 911, 913. Plaintiffs' retention claims must be dismissed for lack of Article III standing.

C. Collection of Face Scans

The much closer question on standing is whether Plaintiffs suffered a concrete injury arising from Google's creation of their face templates without their knowledge.[12] Viewing the facts in the light most favorable to Plaintiffs, they did not know Google created their face templates based on the photos of Plaintiffs' faces uploaded to Google Photos. *See* Pls. Resp. Def. SOF ¶ 29 (quoting Weiss Dep. Tr. at 171:21 ("I would not have consented if I had known that biometric information was

[12]To be crystal clear, the Court reiterates that it is assuming for purposes of this Opinion that Plaintiffs' face templates are biometric identifiers or information as defined by the Act, 740 ILCS 14/10, and that Google did not provide the required disclosures or obtain the required consent, *id.* § 14/15.

being gathered, collected, stored.")); Pls. Statement of Add. Facts ¶ 2 (quoting Rivera Dep. Tr. at 9:9-13 "[Ms. Gutierrez] stated that if I was aware that Google had this face recognition where they were using biometric information, which is a template of my face, so whenever my phot[o]s were taken with her device, they were automatically uploaded. I was then upset, very angry at the fact that they were taken without my consent and I didn't have any control as to whether or not they were able to be used.")).

Gubala does not directly answer this issue because here Plaintiffs did not know that their face templates were being created by Google. Google argues otherwise, contending that "[i]t makes no difference that *Gubala* referred to 'retention' of data, while Google here is alleged to have impermissibly obtained and retained the face templates." Def.'s Br. at 11. But *Gubala* did not merely "refer" to retention of private information—instead, retention was the limit of the holding, because the cable subscriber *knew* that Time Warner had his information. In fact, the subscriber himself provided the information when signing up for cable service. 846 F.3d at 910. The same fact—that the plaintiffs knew or should have known that their biometric information was being collected by the defendant—also distinguishes other district court cases relied on by Google. *See, e.g.*, *Howe v. Speedway LLC*, 2018 WL 2445541, at *6 (N.D. Ill. May 31, 2018) (plaintiff's "fingerprints were collected in circumstances under which any reasonable person should have known that his biometric data was being collected."); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 515 (S.D.N.Y. 2017), *aff'd in relevant part, vacated in part, remanded sub*

nom. Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017) ("The allegations show that the plaintiffs, at the very least, understood that Take-Two had to collect data based upon their faces in order to create the personalized basketball avatars, and that a derivative of the data would be stored in the resulting digital faces of those avatars so long as those avatars existed."). Here, Plaintiffs did not knowingly place their finger on a fingerprint scanner (as in *Howe*) or stare up-close at a camera for about 15 minutes while a camera scanned their face and heads (as in *Vigil*, 235 F. Supp. 3d at 505). Instead, they merely took pictures of themselves (or allowed them to be taken), which then were automatically uploaded to Google Photos where their face template was created. So *Gubala*, *Howe*, and *Vigil* are not directly on point when evaluating the extent of the privacy intrusion of Google Photos.

On the flip side, however, recent cases that have found Article III standing where the plaintiff *did not know* of the collection of biometric information are themselves also not directly on point, because in those cases the information was then disclosed to a third-party. In two recent cases, plaintiffs have successfully shown injury-in-fact because the defendant disclosed a fingerprint scan to a third-party without informing the plaintiff or obtaining the plaintiff's consent. *See Miller v. Sw. Airlines Co.*, 2018 WL 4030590, at *3 (N.D. Ill. Aug. 23, 2018); *Dixon v. Washington & Jane Smith Cmty.-Beverly*, 2018 WL 2445292, at *10 (N.D. Ill. May 31, 2018). Although the opinions included dicta suggesting that collection of biometric data without the plaintiff's knowledge can constitute a concrete risk of harm, ultimately the courts relied on both the absence of consent in collection of the fingerprint *and*

the later disclosure of the fingerprint without consent *Miller*, 2018 WL 4030590, at *3 ("A violation of [the Act's] notice and consent provisions does not create a concrete risk of harm to a plaintiff's right of privacy in his or her biometric data unless the information is collected or *disseminated without the plaintiff's knowledge or consent*.") (emphasis added); *Dixon*, 2018 WL 2445292, at *9 ("Obtaining or *disclosing* a person's biometric identifiers or information *without her consent or knowledge* necessarily violates that person's right to privacy in her biometric information.") (emphasis added). As discussed earlier, Plaintiffs concede that their face templates have not been shared—and there is no showing that there is an imminent risk that they will be shared—with anyone outside of Google. Pls. Resp. Def. SOF ¶¶ 47, 49-52. So the two district-court decisions are not directly applicable to this case.

As the parties discuss in detail, the most factually analogous case is *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018).[13] In *Patel*, the plaintiffs alleged that Facebook applies facial-recognition software to pictures uploaded by users, and then creates and stores face templates based on geometric relationships of facial features—all without users' consent. *Id.* at 951. The plaintiffs did not allege any injury (such as emotional distress, physical harm, dissemination to a third-party, or adverse employment impacts) beyond the violation of the Act's notice-and-consent requirements. *Id.* at 951, 954; *see also* Amend. Compl., *In re Facebook Biometric Info. Privacy Lit.*, No. 3:15-cv-03747, R. 40 (N.D. Cal. Aug. 28, 2015). The district court

[13]On May 29, 2018, the Ninth Circuit granted Facebook's petition for interlocutory appeal of the district court's order granting class certification. *Patel v. Facebook, Inc.*, USCA No. 18-15982 (9th Cir. May 30, 2018). No oral argument has been scheduled yet.

denied Facebook's motion to dismiss for lack of standing, holding that the plaintiffs had sufficiently alleged a concrete injury to satisfy Article III based solely on the violation of the Act. *Patel*, 290 F. Supp. at 956.

Patel placed great weight on the legislative findings and intent underlying the Act, and indeed (and as discussed above) *Spokeo* does instruct courts to respect legislative judgments in identifying intangible harms. As recounted by *Patel*, the Illinois legislature found that (1) biometrics are uniquely sensitive and when compromised, put individuals at a heightened risk for identity theft; (2) biometric technology is cutting edge, and "[t]he full ramifications of biometric technology are not fully known"; (3) the public is "weary"[14] of using biometrics when tied to personal information; and (4) regulating biometric collection, use, and storage serves the public interest. *Id.* at 953 (citing 740 ILCS 14/5(b)-(e), (g)). The district court reasoned that these legislative findings, combined with the notice-and-consent requirements (among other requirements of the Act), left "little question that the Illinois legislature codified a right to privacy in personal biometric information" and that the legislature determined "that a violation of [the Act's] procedures would cause actual and concrete harm." *Id.*

Because a statutory violation is not *necessarily* enough for Article III standing, it is important to discern exactly on what grounds *Patel* relied for finding concrete harm. *Patel* appears to rely on two specific points: first, as the Illinois legislature found, biometric information "cannot be changed if compromised or misused." *Id.* at

[14] It is possible that the word "weary" in the Act, 740 ILCS 14/5(d), was intended to be "wary."

954. So when there is a violation of the Act, *Patel* asserted, "the right of the individual to maintain her biometric privacy vanishes into thin air." *Id.* Second, later in the opinion, *Patel* distinguished two cases that had rejected standing under the Act. In those two cases, the plaintiffs knew that their biometric information was being collected by the defendants. *Id.* at 955 (discussing *Vigil*, 235 F. Supp. 3d at 513 (scans of plaintiffs' faces that took 15 minutes and required plaintiffs to consent by pressing "continue" after reading a notice stating a "face scan" might be recorded); and *McCullough v. Smarte Carte, Inc.*, 2016 WL 4077108 (N.D. Ill. Aug 1, 2016) (plaintiffs scanned their fingerprints to rent a locker)). *Patel* explained that the injuries there were not sufficiently concrete because the plaintiffs "indisputably knew that their biometric data would be collected before they accepted the services offered by the businesses involved." *Patel*, 290 F. Supp. 3d at 955. So *Patel*'s holding stands on two pillars: the risk of identity theft arising from the permanency of biometric information, as described by the Illinois legislature, and the absence of in-advance consent to Facebook's collection of the information. *Id.*

This is a close question, but even when drawing all inferences in Plaintiffs' favor, neither pillar supports a finding of concrete injury. First, as discussed in detail earlier, there is no evidence of a substantial risk that the face templates will result in identity theft. It is true that if an unintended disclosure happens, then there are few ways to change biometric information, and federal courts should follow the legislature's lead in considering that immutability in deciding what is a "substantial" risk. But even taking that permanency into account does not justify an across-the-

board conclusion that *all* cases involving *any* private entity that collects or retains individuals' biometric data present a sufficient risk of disclosure that concrete injury has been satisfied in *every* case.

On the second pillar of *Patel*, there is no legislative finding that explains why the absence of consent gives rise to an injury that is *independent* of the risk of identity theft. *See* 740 ILCS 14/5(a)-(g). Indeed, the only specific injury described by the Act's findings is the risk of identity theft, 740 ILCS 14/5(c), (d). The other findings only set forth broad conclusions, like the "public welfare, security, and safety will be served" and the "full ramifications of biometric technology are not fully known." 740 ILCS 14/5(f), (g). The generality of the legislature's findings is especially damning when considering whether unconsented face scans are sufficiently concrete for Article III purposes. Most people expose their faces to the general public every day, so one's face is even more widely public than non-biometric information like a social security number. Indeed, we expose our faces to the public such that no additional intrusion into our privacy is required to obtain a likeness of it, unlike the physical placement of a finger on a scanner or other object, or the exposure of a sub-surface part of the body like a retina. There is nothing in the Act's legislative findings that would explain why the injury suffered by Plaintiffs here—the unconsented creation of face templates—is concrete enough for Article III purposes. As important and instructive as legislative judgments are in evaluating intangible harms, the Act does not support a finding that the concrete-injury requirement has been met in this case.[15]

[15]This holding is limited to the specific circumstances of this case, which challenges face scans. Likewise, this holding of course does not preclude the legislature from making

Moving on from legislative findings, *Spokeo* instructs courts to also examine possible analogues to common law harms that historically have supported a finding of Article III injury-in-fact. *Spokeo*, 136 S. Ct. at 1549 ("[I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.") In this case, Plaintiffs' response brief outlines the historical development of the right to privacy in American law, which was "fueled by social and technological change." Pls.' Resp. Br. at 8. They argue that the Act directly follows from common law privacy torts. *Id.* at 8-9. It is true that the alleged injury in this case need not square on all fours with a common law privacy tort. Plaintiffs are correct that they do not have to adequately state a claim under a common law tort; otherwise, they would just pursue a common law claim, and *Spokeo* must have meant more than that when it authorized claims for harms that bear a close relationship to common law claims. Pls.' Resp. Br. at 10; *see also Whitaker v. Appriss, Inc.*, 229 F. Supp. 3d 809, 813 (N.D. Ind. 2017) (noting that the "close relationship" test does not require "sameness"). At the same time, however, the common law tort must bear a close relationship to the alleged injury in *this* case in order for the common law analogue to be instructive. *See Spokeo*, 136 S. Ct. at 1549; *see also Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (statutory violation led to "unsolicited

---

additional findings either now or in the future. It is not hard to imagine more concrete concerns arising from facial-recognition technology, especially as it becomes more accurate and more widespread (along with video-surveillance cameras) to the point that private entities are able to use the technology to pinpoint where people have been over extended time periods.

contact" and "disturb[ing of] solitude," similar to nuisance tort); *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1114-15 (9th Cir. 2017) (statutory violation resulted in "dissemination of false information," similar to defamation tort).

To start, there are four well-established common law privacy torts: (a) unreasonable intrusion upon someone's seclusion; (b) appropriation of a person's name or likeness; (c) unreasonable disclosure of private facts; and (d) publicity that unreasonably places the other in a false light. Restatement (Second) of Torts § 652A (1977). Plaintiffs rightly do not argue that Google's alleged conduct is anything like the public disclosure of private facts or false-light invasion of privacy. Pls.' Resp. Br. at 8-10. That leaves intrusion on seclusion and appropriation of likeness.

Starting with intrusion on seclusion, the Second Restatement of Torts defines this tort as a claim against someone "who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns … if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (1977). The elements of the tort are "(1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is highly offensive or objectionable to a reasonable person; (3) that the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering." *Jacobson v. CBS Broad., Inc.*, 19 N.E.3d 1165, 1180 (Ill. App. Ct. 2014). The third element, that the intrusion be upon a *private* matter, is a necessary predicate for the other elements. *Id.* at 1181; *see also Lovgren v. Citizens First Nat. Bank of Princeton*, 534 N.E.2d 987, 989 (Ill. 1989) ("[T]he core of this tort is the

offensive prying into the *private* domain of another.") (emphasis added). It is this element where the relationship between Plaintiffs' alleged injury and this common law tort breaks down.

First, Plaintiffs cannot show—and do not argue—that Google "intruded into a private place" by receiving photographs of Plaintiffs voluntarily uploaded (by Weiss or Gutierrez) to Google Photos. *See* Pls.' Resp. Br. at 8-11; R. 60, Opinion 2/27/17 at 26 n.11 ("Neither side is arguing that for the purposes of the Privacy Act, Google needed consent to upload the photographs to the cloud."). Second, although Plaintiffs argue that their faces are not public, Pls.' Resp. Def.'s SOF ¶ 60 (disputing "that their faces are public, not private."), Plaintiffs' only evidence to support that assertion is deposition testimony in which they say that their facial *biometrics* are private information. *Id.* (quoting Weis Dep. Tr. at 183:18-19 ("Looking [at someone's face with your eyes] and recording [someone's face with biometric identifiers] are different, as far as I understand."); quoting Rivera Dep. Tr. at 45:15-19 ("[W]hen it's taking my biometric information, that's sensitive information to me. That's my personal information.")). Plaintiffs do not offer evidence to dispute that their *faces* are public—just that their facial *biometrics* are. This is consistent with Fourth Amendment case law that rejects an expectation of privacy in a person's face. *See United States v. Dionisio*, 410 U.S. 1, 14 (1973) (explaining that "[n]o person … can reasonably expect that his face will be a mystery to the world," and holding that an individual's face, when knowingly exposed—even in his own home or office—is not protected by the Fourth Amendment) (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)). Indeed,

Illinois courts have dismissed many intrusion-upon-seclusion claims that were premised on photographs or videos for failure to satisfy the privacy element of the tort. *See Jacobson*, 19 N.E. at 1181 (affirming dismissal where plaintiff was filmed on "readily visible property" and the images of her revealed nothing that was "especially private"); *Schiller v. Mitchell*, 828 N.E.2d 323, 326, 329 (Ill. App. Ct. 2005) (defendants did not intrude upon plaintiffs' seclusion by capturing surveillance video of plaintiffs on their property, including within their garage, because passersby could see the same things from different angles); *see also* Restatement (Second) of Torts § 652B cmt. c (there is no intrusion-upon-seclusion liability for "observing [a plaintiff] or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye"). It bears repeating that Plaintiffs need not satisfy the elements of a common law tort to show Article III injury. But there is a wide gap between the alleged injury here—the creation and retention of the face templates—and the privacy interest protected by the intrusion-on-seclusion tort. All that Google did was to create a face template based on otherwise public information—Plaintiffs' faces. *See Patel v. Zillow, Inc.*, 2017 WL 3620812, at *10 (N.D. Ill. Aug. 23, 2017) (defendant did not intrude into private matters when it created real-estate data derived from public information).

Another element of the intrusion-on-seclusion tort shows the disconnect between the common law claim and this case: the creation of face templates is not a "highly offensive" intrusion.[16] As discussed earlier, the templates are based on

[16]Plaintiffs argue that whether the creation of face templates was "highly offensive" would "clearly be for a jury to decide at trial, not for the Court to decide at summary

something that is visible to the ordinary eye, that is, Plaintiffs' faces. And the crux of the tort is the intrusion itself, not what is done with the fruits of the intrusion (if there are any fruits) later. In other words, "[t]he basis of the tort is *not* publication or publicity." *Lovgren*, 534 N.E.2d at 989 (emphasis added). So what Google did with the photographs of Plaintiffs' faces—that is, using them to create face templates—is irrelevant when comparing this case to an intrusion-on-seclusion claim. In any event, the record shows that Google only used the facial images to create face templates that organize Plaintiffs' photographs in private Google Photos accounts. Plaintiffs do not present any evidence showing that Google commercially "exploited" their faces or the face templates they created. Without more, Plaintiffs' injury in this case does not bear a close relationship to the tort of intrusion upon seclusion.[17]

That leaves the tort of appropriation of likeness. This common law tort protects an individual's "interest … in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or others." Restatement (Second) of Torts § 652C cmt. a (1977).[18] This interest is

---

judgment." Pls.' Resp. Br. at 10. If Plaintiffs asserted the intrusion-on-seclusion claim, then that argument would have greater force, because the merits of the claim could be a question for the jury. But the analysis at hand is whether Plaintiffs have sufficiently established an injury-in-fact under Article III for purposes of subject matter jurisdiction. There is no general Seventh Amendment jury trial right for issues of subject matter jurisdiction, and Plaintiffs offer no precedent that the close-relationship analysis, as explained in *Spokeo*, is a matter for the jury to decide.

[17]Plaintiffs' argument that the creation of face templates is similar to "restaurants [] dust[ing] their customers' glasses for fingerprints and stockpil[ing] those identifiers," Pls.' Resp. Br. at 10, is misplaced. Fingerprints are not held out to the public like faces, which are visible to the ordinary eye. Applying a template to a face on a voluntarily uploaded photograph is very different from collecting the tiny physical remnants left by ridges on a person's fingers.

[18]In Illinois, the common law tort of appropriation of likeness was replaced with the Right of Publicity Act, 765 ILCS 1075/30, effective in 1999. *Trannel v. Prairie Ridge Media,*

invaded when a defendant uses the likeness "to advertise [its] business or product," "for some similar commercial purpose," or "for [its] own purposes and benefit." *Id.* cmt. b. Plaintiffs have not shown that Google has done anything closely related to appropriation of their likenesses. In their Rule 56.1 Statement, Plaintiffs dispute that "[t]here is no evidence that any of the data generated by Google Photos was used in any way except to help organize the photographs in Wiess's and Gutierrez's accounts." Pls. Resp. Def. SOF ¶ 59; *see also* Pls. Statement Add. Facts ¶ 6. But the evidence offered in their response fails to adequately support their denial. Plaintiffs cite to an article that describes ways in which Google's facial recognition technology *could* be used in the future, including data mining, targeted advertisements, and filtering content, Pls. Statement Add. Facts ¶ 6 (citing Maya Decl., Exh. K), as well as an email chain among Google employees forwarding an article discussing similar "likely" uses, *id.* (citing Maya Decl., Exh. I). These exhibits only demonstrate *future* potential uses of Google's facial recognition technology; they do not suggest that Google currently employs these practices, that Google likely will do so in the future without consent, or that Google used Plaintiffs' data in this way. So the evidence falls well short of a substantial likelihood that Plaintiff's will suffer any of those injuries. The only other tack that Plaintiffs could possibly take is to argue that Google "mapped Plaintiffs' faces, creating, collecting, storing, and exploiting their unique biometric identifiers for its own competitive advantage in the marketplace for photo-sharing services." Pls.'

Inc., 987 N.E.2d 923, 929 (Ill. App. Ct. 2013). The Act has nearly identical elements to the common law tort, and a plaintiff must allege three elements: "(1) an appropriation of one's name or likeness; (2) without one's consent; and (3) for another's commercial benefit." *Id.*

Resp. Br. at 2. But Plaintiffs do not develop this argument or offer evidence in support of it. Google's use of the face templates for the sole purpose of organizing photographs does not bear a "close relationship" to harms caused by appropriation of likeness.

With neither a legislative judgment nor a common law analogue (or anything else) to support a finding of concrete injury, the Court concludes that Plaintiffs have not demonstrated an injury-in-fact sufficient to confer Article III standing.[19] This case presented close legal questions, which is not uncommon when it comes to technological advances,[20] and the Court appreciates the able presentations of both sides.

IV. Conclusion

Google's motion for summary judgment is granted. The Court lacks subject matter jurisdiction because Plaintiffs have not suffered concrete injuries for Article III purposes. In light of that holding, there is no need to opine on the statutory-interpretation arguments (and, in any event, the Illinois Supreme Court has the issue

[19]A court within this District held the plaintiff had alleged an injury-in-fact where the defendant allegedly collected his face scans without his knowledge in violation of the Act. *Monroy v. Shutterfly*, 2017 WL 4099846, *8 n.5 (N.D. Ill. Sept. 15, 2017). But *Monroy* relies on a generally described privacy invasion, rather than engage in an analysis of specific common law torts (it also does not appear that the parties precisely teed up this issue for the district court in that case, as the defendant did not challenge the plaintiff's standing). *Id.*

[20]The difficulty in predicting technological advances and their legal effects is one reason why legislative pronouncements with minimum statutory damages and fee-shifting might reasonably be considered a too-blunt instrument for dealing with technology. Of course, there might be policy considerations that weigh in favor of taking the broader approach.

under advisement). The case is dismissed for lack of subject matter jurisdiction and the status hearing of January 22, 2019 is vacated.

ENTERED:

s/Edmond E. Chang
Honorable Edmond E. Chang
United States District Judge

DATE: December 29, 2018