Designing Privacy Policies and Identifying Privacy Risks for Financial Institutions

June 2016

Dechert LLP

Program Overview

- Regulatory Environment
- Who Needs a Privacy Program and Common Questions
- Components of a Comprehensive Privacy Program
- Tailoring, Implementing and Monitoring Your Privacy Program
- Understanding Contractual Liabilities
- Key Takeaways from OCIE's September 15, 2015 Risk Alert
- Recent SEC Enforcement Actions

Key Statutes And Regulations

- Federal Laws
  - Title V of the Gramm-Leach-Bliley Act of 1999
  - Regulation S-P
  - FTC Privacy of Consumer Financial Information Rule ("FTC Privacy Rule")
  - FTC Standards for Safeguarding Customer Information ("FTC Safeguards Rule")
  - Regulation S-AM
  - Regulation S-ID
  - FTC Act Section 5

- State Laws
  - Massachusetts Standards for the Protection of Personal Information
    - 201 CMR 17, et. Seq.
  - California Online Privacy Protection Act ("CalOPPA")

Basis For Liability

- FTC Act Section 5
- SEC/FTC Enforcement Actions
- Litigation
- State AG Enforcement Actions

Who Needs a Privacy Program?

- **In General: Any financial institution that obtains nonpublic personal information from its customers needs a privacy program.**

- **"Consumer"** means "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative."

- **"Customer"** means "a consumer who has a customer relationship with you."

- **"Nonpublic personal information"** means "(i) personally identifiable financial information; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information."

- **"Personally identifiable financial information"** means any information: "(i) a consumer provides to you to obtain a financial product or service from you; (ii) about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer."

Who Needs a Privacy Program? Common Questions

- I am a registered investment adviser ("RIA") to registered investment companies that have individual, natural person investors.
  - Regulation S-P applies to the adviser and to the funds. The adviser on its own behalf (and on behalf of the funds) needs a privacy program.
- I am a RIA, but the registered investment companies I manage only have institutional investors.
  - Reg. S-P and the FTC Privacy Rules do not apply to information relating to institutional investors or pension funds. The RIA and the funds do not need a privacy program.
- I am a RIA and private fund manager. My clients (for purposes of Form ADV) are the private funds I manage. High net worth individuals invest in those funds.
  - The FTC Privacy Rules are broad enough to encompass private funds and Reg. S-P applies to the adviser. Both need a privacy program.
- I am a RIA, but the individual investors in the funds I manage are non-U.S. persons. I conduct activities only through non-U.S. offices and branches.
  - Reg. S-P explicitly applies. The adviser needs a privacy program.
- I am an investment adviser, and I manage individual investors' money. I am not registered with the SEC.
  - The FTC Privacy Rules are broad enough to encompass non-registered advisers. The adviser needs a privacy program.

Components of a Privacy Program

- Privacy Programs have a number of components, including a:
  - Privacy Notice
    - Regulation S-P and the FTC Privacy Rule
  - Written Information Security Program
    - Regulation S-P and the FTC Privacy Rule
  - Regulation S-AM Notice
    - Regulation S-AM
  - Red Flags Program
    - Regulation S-ID
  - Online Privacy Policy
    - California Online Privacy Protection Act (“CalOPPA”)
  - Incident Response Plan
    - SEC Guidance; SEC Cybersecurity Examination Initiative; SEC Enforcement Order
- Whether a given entity needs all, or only some, of the listed components depends on that entity’s specific business practices.

Privacy Notice – Generally (Reg. S-P / FTC Privacy Rule)

- Regulation S-P and the FTC Privacy Rule require financial institutions to provide customers with initial and annual privacy notices with respect to their sharing of nonpublic personal information with affiliates and unaffiliated third parties.

- When the financial institution shares consumer information in certain ways, these notices also must provide a reasonable opportunity for the consumer to “opt out” of having the consumer’s information shared.

Privacy Notice – Who needs to provide one? (Reg. S-P / FTC Privacy Rule)

Financial institutions are required to provide **customers** with initial and annual privacy notices with respect to their sharing of **nonpublic personal information** with affiliates and unaffiliated third parties.

- "**Financial institution"** means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). Under the FTC Privacy Rule, it means a business "significantly engaged" in "financial activities" under section 4(k) of the Bank Holding Company Act.

- **"Consumer"** means "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative."

- **"Customer"** means "a consumer who has a customer relationship with you."

- **"Customer relationship"** means "a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes."

- **"Nonpublic personal information"** means "(i) personally identifiable financial information; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information."

- **"Personally identifiable financial information"** means any information: "(i) a consumer provides to you to obtain a financial product or service from you; (ii) about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer."

Privacy Notice – Timing and Content (Reg. S-P / FTC Privacy Rule)

- A notice and opt-out form must be provided at the time a customer relationship is formed, and then annually thereafter
- SEC/FTC take the view that you violate Reg. S-P by sharing information ***before*** disclosure and opportunity to opt-out.
- The SEC/FTC have not been aggressive about enforcing this, yet.

SAMPLE PRIVACY NOTICE

FACTS	WHAT DOES COMPANY DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social Security number and assets ▪ Investment experience and risk tolerance ▪ Account transactions and wire transfer instructions
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Company chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Company share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes— to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes— information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes— information about your creditworthiness	Yes	Yes
For nonaffiliates to market to you	Yes	Yes
To limit our sharing	• Call us. • Visit us online **Please note:** If you are a *new* customer, we can begin sharing your information **in 30** days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our	
Questions?	Call us or go to Company's website.	

Privacy Notice – A Key Practice Point (Reg. S-P / FTC Privacy Rule)

- Financial institutions must abide by the policies set out in the privacy notices they deliver.

Written Information Security Program ("WISP") (Reg. S-P / FTC Safeguards Rule)

- Reg. S-P and the FTC Safeguards Rule also require financial institutions to "adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."

- The policies and procedures must be "reasonably designed" to:
  - "Insure the security and confidentiality of customer records and information;
  - "Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
  - "Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

- What does this mean and how do you do it?
  - Many U.S. firms look to the Massachusetts Standards for the Protection of Personal Information (the "Massachusetts Standards") for guidance.
  - Require administrative, physical and technical safeguards.

Written Information Security Program ("WISP") Massachusetts Standards: Administrative Safeguards

- Designated employee to maintain information security program;
  - At least annual review of Program; Monitoring security Program
- Identify and assess reasonably foreseeable internal and external risks;
- Develop security policies for employees that account for which employees have access to information
- Employee training and employee disciplinary procedures
- Third Party Service Provider Verification

Written Information Security Program ("WISP") Massachusetts Standards: Technical Safeguards

- Numerous technical requirements including:
  - Secure user IDs and other identifiers;
  - Secure access control measures;
  - Encryption of both (1) laptops, and (2) other portable devices;
  - System monitoring;
  - Firewall protection;
  - Up-to-date patches and virus definitions; and
  - Education and training
- Conduct gap analysis – inventory all current I.T. procedures and identify any deficiencies

Regulation S-AM Notices: Generally

- Adopted by the SEC in 2010
- Applies to brokers, dealers, investment companies, registered investment advisers, and registered transfer agents ("S-AM Institutions")
- Governs the ability of S-AM Institutions to use certain consumer information obtained from their affiliates to make marketing solicitations
- Regulation S-AM applies only when an S-AM entity *uses* information obtained from an affiliate, unlike Regulation S-P, which governs information *sharing*

Regulation S-AM Notices: Requirements

- An S-AM Institution may not use eligibility information about a consumer received from an affiliate to make “marketing solicitations” to customers unless:
  - The consumer has received notice;
  - The consumer has a reasonable chance to opt-out; and
  - The consumer did not opt out
- A marketing solicitation is any communication made to a consumer based on eligibility information that is intended to encourage the consumer to buy a product or use a service offered by the marketer

Regulation S-AM Notices: Exceptions

- There are six exceptions to Regulation S-AM for persons that receive eligibility information from an affiliate:
  - To make a marketing solicitation to a consumer with whom the person has a pre-existing business relationship;
  - To facilitate communications to an individual for whose benefit the person provides employee benefit or other services pursuant to a contract with an employer related to and arising out of the current employment relationship or status of the individual as a participant or beneficiary of an employee benefit plan;
  - To perform services on behalf of an affiliate (subject to certain exceptions);
  - In response to a communication about its product and services initiated by the consumer;
  - In response to solicitations authorized or requested by the consumer; or
  - If compliance would conflict with applicable provisions of state insurance laws pertaining to unfair discrimination.
- Generally, the preexisting business relationship is the most useful.

Regulation S-AM Notices: Exceptions

- An S-AM Institution will not need to comply with Regulation S-AM in connection with making solicitations to consumers with whom the institution has a preexisting business relationship, which is defined as a relationship based on:
  - A financial contract in force at the time the marketing
  - A financial transaction (including an active account) within 18 months preceding the date of the marketing;
  - An inquiry or application by the consumer regarding a product or service during the three months preceding the date the marketing solicitation.
- For example, if a consumer has an account with an adviser and also deposit at an affiliated bank, the adviser may use eligibility information obtained from the bank to market additional products or services to the consumer without having to provide notice or an opportunity to opt-out.

Regulation S-AM: Notice and Opt-Out Requirements

- If Regulation S-AM applies, an S-AM Institution must send customers an initial notice that is clear, conspicuous and concise
- The notice must disclose:
  - A list of the affiliates or types of affiliates whose use of eligibility information is covered by the Notice;
  - A general description of the types of eligibility information that may be used;
  - That the consumer may elect to limit the use of eligibility information to make marketing solicitations to the consumer;
  - That the consumer's election will apply for a specified period of time stated in the Notice and, if applicable, that the consumer will be allowed to renew the election once that period expires;
  - If the Notice is provided to consumers who may have previously opted out, such as if a Notice is provided to consumers annually, that the consumer who has chosen to limit solicitations does not need to act again until the consumer receives a renewal notice; and
  - A reasonable and simple method for the consumer to opt out.

Regulation S-AM Notices: Delivery

- Regulation S-AM permits an S-AM Institution to combine Regulation S-AM notices with Regulation S-P notices.
- This would probably be most useful where the institution plans to send annual Regulation S-AM notices.

Red Flags Rule: Overview (Regulation S-ID)

- Regulation S-ID (the “Red Flags Rule”) requires “financial institutions” and “creditors” to:
  - Establish a written, board approved Identity Theft Program;
  - Identify “red flags” of identity theft – any “pattern, practice, or specific activity that indicates the possible existence of identity theft”;
  - Detect “red flags”;
  - Prevent and mitigate identity theft;
  - Update the Identity Theft Program; and
  - Administer the Program.
- Guidelines suggest oversight of the Program by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management.

Red Flags Rule: Triggers (Regulation S-ID)

- "Financial Institution" is a bank, credit union, or any other person that holds a "transaction account"
  - "Transaction Account" is generally considered a deposit or account on which the depositor or account holder is permitted to make withdrawals for the purpose of making payments to third parties.
- "Creditor" is defined broadly as any entity or person who regularly arranges for, extends, renews or continues credit
  - Interpreted expansively; includes any situation in which services or goods are provided prior to receipt of full payment
  - Creditor may include lenders such as banks, brokers, finance companies, auto dealers, mortgage brokers, utility companies, telecommunications companies, and professional services providers
- "Covered Account" is an account primarily for personal, family, or household purposes that is designed to permit multiple payments or transactions to third parties; or any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft

Red Flags Rule: Identifying Red Flags (Regulation S-ID)

- Analyze and inventory all past data security threats
  - Industry alerts, customer notifications or concerns, presentation of suspicious documents, unusual account activity, etc. should all be considered “red flags” of identity theft
- Analyze and inventory past responses to such incidents
  - Have remedial technical measures been implemented?
  - Were past notification procedures effective?
  - Were accounts monitored?
- Create matrix of all sources of personal information, and how that information is maintained
  - Assess vulnerabilities: How long is information stored, how is it stored, who has access to the information, is more sensitive information stored in a secure environment?
- Analyze threats to current maintenance and overview procedures

Red Flags Rule: Prevention and Mitigation (Regulation S-ID)

- Prepare incident response protocol
  - Incident response should dependent on type of threat, incident, information involved, etc.
  - Match response to type of threat/risk/sensitive information
    - Monitor account for unusual activity, contact customer, change passwords, shut down account, notify law enforcement, etc.
- Rule does not mandate specific technical requirements
- Document all incidents, responses, and outcomes. Administer and update program accordingly

Online Privacy Policy (California Online Privacy Protection Act)

- Companies that use websites to engage with their customers need to have an online privacy policy

- Policies should be drafted in accordance with the California Online Privacy Protection Act

- Online privacy policies explain:
  - The categories of personal information collected about users via the website
  - The categories of third parties with whom that information is shared
  - Any opportunities that consumers may have to opt out of that information sharing
  - Whether the website employs data collection technologies, such as cookies or other tracking technologies
  - How the company's website responds to "do not track" signals it receives from browsers
  - Whether "other parties" may collect personal information about a website user when the collection is done over time and across different websites

Incident Response Plan

- An incident response plan details, in writing, a concrete plan for what a company will do if it faces a suspected or actual data breach or cyber-attack. The plan should, at a minimum:
  - Identify the company's most vulnerable data;
  - Assign responsibility for each element of the response plan and provide 24-hour contact information for all personnel and back-up personnel;
  - Explain how to determine whether an incident is actually a breach and whether and how it should be escalated;
  - Indicate that data should be preserved so that a forensic investigation can be conducted;
  - Identify who will keep logs and records of all information relating to the incident; and
  - Include procedures for notifying law enforcement and criteria for whether customers or third-parties need to be notified.
- Incident response plans should be tested
  - Personnel need to be trained and know how to respond to a data breach or cyber-attack.

Tailoring Your Program: Data Flows

- How is personal data obtained, directly or indirectly?
- Where is the data held?
- How long is data kept?
- How is data used?
- Who has access to data?
  - Employees
  - Affiliates
  - Third Parties: vendors, service providers
- What data is shared with business partners?

Implementing Your Program

- Firms must actually implement the policies and procedures they adopt.
  - Firms should conduct periodic assessments, create a strategy designed to prevent, detect and respond to cybersecurity threats, and "***Implement the strategy through written policies and procedures and training*** that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.

    SEC IM Guidance Update, Cybersecurity Update, April 2015
  - "[P]ublic reports have identified cybersecurity breaches related to weaknesses in basic controls. As a result, ***examiners*** will gather information on cybersecurity-related controls and ***will also test to assess implementation of certain firm controls***."

    OCIE 2015 Cybersecurity Examination Initiative, September 2015
  - R.T. Jones "failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule." "***To mitigate against any future risk of cyber threats, R.T. Jones has*** appointed an information security manager to oversee data security and protection of PII, and ***adopted and implemented a written information security policy***" as a remedial effort.

    SEC Order, R.T. Jones Capital Equities Management, Inc., September 22, 2015

Testing and Monitoring Your Program

- Firms should continually monitor their vulnerabilities and conduct regular evaluations to ensure their policies and procedures are working.
  - "Create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Routine testing of strategies could also enhance the effectiveness of any strategy."

    SEC IM Guidance Update, Cybersecurity Update, April 2015
  - "***Examiners also may assess whether firms are periodically evaluating cybersecurity risks*** and whether their controls and risk assessment processes are tailored to their business."

    OCIE 2015 Cybersecurity Examination Initiative, September 2015
  - R.T. Jones "failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule. ***R.T. Jones's procedures for protecting its clients' information did not include, for example: conducting periodic risk assessments*** . . ."

    SEC Order, R.T. Jones Capital Equities Management, Inc., September 22, 2015

The “Downstream Effects” of Reg. S-P / FTC Privacy Rules: Step I

- If you, as a financial institution, receive nonpublic personal information from a nonaffiliated financial institution under an exception to the notice and opt out requirements, your disclosure is limited.
- You essentially “step into the shoes” of the disclosing entity, and must limit your sharing the same way the disclosing entity does.
- Familiarize Yourself with Your Current Agreements
  - If you receive nonpublic personal information from other financial institutions you may be contractually required to protect it in very specific ways.

The “Downstream Effects” of Reg. S-P / FTC Privacy Rules: Step II

- You may also share nonpublic personal information with non-financial institutions, such as vendors and third-party service providers
- Raises liability issues for you (the disclosing entity) because you are obligated to ensure down-stream protection of nonpublic personal information
- Consider that service providers and third party vendors may not be subject to the relevant laws

Dealing with Third-Party Vendors / Service Providers

- Conduct due diligence with regard to vendor selection
- Hold service providers to the same legal standard
- Require service providers to provide notice of security breaches
- Supervise and monitor service providers' compliance

Model Provisions: Contracts with Third-Party Vendors / Service Providers

- Maintain confidentiality and comply with applicable law
  - "Confidential Information" shall include, but not be limited to, any or all of the following: (a) the names, addresses, telephone, facsimile numbers, financial data, e-mail addresses, and any other "Non-Public Personal Information" as that term is used in the Gramm-Leach-Bliley Act of 1999 (the "Act"), regarding Bank's, its operating subsidiaries, or its affiliates' customers, or prospective customers. . .
- Consider that service provider may not be subject to the relevant laws
- Service provider may have different security standards

Holding Service Provider to Same Legal Standard

- Contractor acknowledges that (1) Bank is subject to the consumer and customer privacy provisions of the Gramm Leach Bliley Act and Federal regulations that implement the Act (the "Regulation"); (2) the Confidential Information covered by this Agreement may include Non-Public Personal Information as defined in the Regulation; and (3) that Bank has certain obligations to protect the Confidential Information from unauthorized disclosure to third parties. Contractor understands that Contractor's willingness and ability to cooperate with and assist Bank in this regard is a material factor in Bank's willingness to enter into this Agreement, and such other agreements as Bank may enter into, or have entered into, with Contractor, through which agreements Confidential Information will be released from Bank to Contractor
- Contractor acknowledges receipt from Bank of a copy of the Gramm-Leach-Bliley Act and acknowledges that it has access to all applicable rules and regulations promulgated thereunder, and warrants that its procedures with regard to preventing release of Confidential Information are such as to be fully compliant with the Regulation as if Contractor were fully subject to the Regulation to the same extent as Bank

Establishing Security Standards for Data Recipients

- Specifically, and not by way of limitation, Contractor shall: (1) maintain Confidential Information of Bank in physical and electronically secure media and facilities, subject to commercially reasonable security procedures; (2) not use, nor permit its employees, agents, subcontractors or affiliates to use, such Confidential Information for any purpose whatsoever except strictly in connection with performance of its contractual duties to Bank; (3) neither use, nor permit use of, such data for any sales or marketing purposes; (4) make and enforce policies and procedures in hiring, training, supervision and monitoring of its staff, agents and subcontractors in proper handling and protection of Confidential Information, including, at a minimum and not by way of limitation, written agreements for confidentiality to be signed personally by all such parties, training, and provision for disciplinary action where appropriate; and (5) not copy, nor permit copying of, the Confidential Information, in any manner, or in any medium, whatsoever, and return all such data immediately upon completion of the task for which it was received, or with Bank's prior written approval, certify destruction of such data in writing

Addressing Security Breaches

- **Notice of Security Breach.** If a party to this Agreement becomes aware of any actual or suspected loss of, unauthorized access to, or unauthorized use or disclosure of any Confidential Information of the other party, including any Personal Information covered by this Agreement, such party promptly shall, at its expense: (a) notify the other party in writing; (b) investigate the circumstances relating to such actual or suspected loss or unauthorized access, use or disclosure; (c) take commercially reasonable steps to mitigate the effects of such loss or unauthorized access, use or disclosure and to prevent any reoccurrence; (d) provide to the Owner such information regarding such loss or unauthorized access, use or disclosure as is reasonably required for the Owner to evaluate the likely consequences and any regulatory or legal requirements arising out of such loss or unauthorized access, use or disclosure; and (e) cooperate with the Owner to further comply with all relevant laws, rules and regulations

OCIE's September 15, 2015 Risk Alert: Key Takeaways

- Unlike OCIE's 2014 Cybersecurity Examination Initiative, OCIE's 2015 Cybersecurity Examination Initiative will focus on whether firms are actually implementing the policies and procedures they have adopted

  - "The staff's document reviews and questions were designed to discern basic distinctions among the level of preparedness of the examined firms. ***The staff conducted limited testing of the accuracy of the responses and the extent to which firms' policies and procedures were implemented***. The examinations did not include reviews of technical sufficiency of the firms' programs."

    OCIE's Cybersecurity Examination Sweep Summary – February 2015

  - "OCIE is issuing this Risk Alert to provide additional information on the areas of focus for OCIE's second round of cybersecurity examinations, which will ***involve more testing to assess implementation of firm procedures and controls***."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015

OCIE's September 15, 2015 Risk Alert: Key Takeaways

- OCIE has indicated that in its 2015 Cybersecurity Examination Initiative, it will drill-down on the specific technical controls firms have in place to protect customer information.
  - "Firms may be particularly ***at risk of a data breach from a failure to implement basic controls*** to prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based on personnel or system changes."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015
  - "Examiners may review how firms control access to various systems and data via management of user credentials, authentication and authorization methods. This may include a ***review of controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation, and tiered access***."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015
  - OCIE may ***request firms' policies and procedures relating to "Patch management practices***, including those regarding the prompt installation of critical patches and the documentation evidencing such actions."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015

OCIE's September 15, 2015 Risk Alert: Key Takeaways

- OCIE's 2015 Cybersecurity Examination Initiative Risk Alert demonstrates an increased focus on "Vendor Management"

OCIE's 2015 Cybersecurity Examination Initiative – September 2015

  - "Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms. As a result, examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor."

OCIE's 2015 Cybersecurity Examination Initiative – September 2015

- This focus on vendor management is particularly interesting due to the following findings reported by OCIE in February 2015:

  - "The vast majority of examined firms conduct periodic risk assessments, on a firm-wide basis, to identify cybersecurity threats, vulnerabilities and potential business consequences***. Fewer firms apply these requirements to their vendors***. A majority of broker-dealers (84%) and ***a third of the advisers (32%) require cybersecurity risk assessments of vendors with access to their firms' networks***."

OCIE's Cybersecurity Examination Sweep Summary – February 2015

In the Matter of R.T. Jones Capital Equities Management, Inc. (September 22, 2015)

- SEC released an Order regarding a settlement with R. T. Jones in connection with its alleged violation of Rule 30(a) of Regulation S-P (the "Safeguards Rule").
- **Alleged Facts:**
  - For approximately 4 years, R. T. Jones—an SEC-registered investment adviser with 8,400 client accounts and $480 million in assets under management–stored sensitive personally identifiable information ("PII") of clients and other persons on its third party-hosted web server.
  - R.T. Jones did not adopt written policies and procedures regarding the security and confidentiality of that information and the protection of that information from anticipated threats or unauthorized access.
  - In July 2013, the firm's web server was hacked and the PII over more than 100,000 individuals, including thousands of R.T. Jones's clients, was left vulnerable to theft.
  - R.T Jones retained more than one cybersecurity consulting firm to confirm and assess the attack. Neither could confirm whether the PII stored on the server had been accessed or compromised.
  - R.T. Jones notified the affected individuals and provided free identity monitoring.
  - At the time of the Order, there was no indication that any client has suffered actual financial harm as a result of the breach.
- **SEC Findings:**
  - R.T. Jones failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule. R. T. Jones's policies and procedures did not include, for example:
    - Conducting periodic risk assessments;
    - Employing a firewall to protect the web server containing client PII;
    - Establishing procedures to respond to a cybersecurity incident; or
    - Encrypting client PII.

In the Matter of Craig Scott Capital, LLC (April 12, 2016)

- SEC released an Order regarding a $100K settlement with Craig Scott Capital, LLC ("CSC"), which arose out of CSC's alleged violation of Rule 30(a) of Regulation S-P (the "Safeguards Rule").

- **Alleged Facts**: From January 2012-June 2014, the staff at Craig Scott Capital-an SEC-registered broker-dealer-used email addresses other than those with the firm's domain name to electronically receive more than 4,000 faxes from customers and other third parties.

  - The Faxes routinely included sensitive customer records and information, such as customer names, addresses, Social Security numbers, bank and brokerage account numbers, copies of drivers' licenses and passports and other customer financial information. Some employees, including the firm's principles, used non-firm email accounts for firm business.

  - In addition, many of the written policies and procedures were not implemented in practice.

In the Matter of Craig Scott Capital, LLC (April 12, 2016)

- **SEC Findings Included the Following**:
  - While CSC had adopted written policies and procedures, which included a section directly addressing the Safeguards Rule, the Staff concluded and charged that the existing policies "were not reasonably designed to protect customer records and information" and indicated that they were not tailored to the actual practices at the firm.
  - The policy stated that the "Designated Supervisor" was responsible for ensuring compliance with the policy, but did not identify the Designated Supervisor.
  - Though CSC used an eFax System, the policy did not address either the eFax System or how to handle the customer records and information contained in eFaxes. As a result, none of the eFaxes received by the non-firm email addresses were maintained and preserved by CSC.
  - The policy contained blanks to be filled in later, such as, "[The Firm] has adopted procedures to protect customer information, including the following [methods]."

In the Matter of Morgan Stanley Smith Barney LLC (June 8, 2016)

- SEC released an Order regarding a $1M settlement with Morgan Stanley Smith Barney ("Morgan Stanley") and an agreement that Morgan Stanley would cease and desist from committing or causing any violations and any future violations of Rule 30(a) of Regulation S-P (the "Safeguards Rule").

- **Alleged Facts**: From at least August 2001 through December 2014, Morgan Stanley stored PII of individuals to whom Morgan Stanley provided brokerage and investment advisory services on two of the firm's applications: the Business Information System ("BIS") Portal and the Fixed Income Division Select ("FID Select") Portal. Galen Marsh (then a Morgan Stanley employee) misappropriated data regarding ~730K customer accounts, associated with ~330K different households by accessing the portals between 2011 and 2014. The data included PII, such as customers' full names, phone numbers, street addresses, account numbers, account balances and securities holdings.

  - Between December 15, 2014 and February 3, 2015, portions of the stolen data were posted for sale on at least three Internet sites. Morgan Stanley discovered the breach through one of its routine Internet sweeps on December 27, 2014 and identified Marsh as the likely source of the breach. Marsh admitted to storing the data on his personal server and a subsequent forensic analysis of the server showed a third party likely hacked into it and copied the customer data that Marsh had downloaded from the Portals.

In the Matter of Morgan Stanley Smith Barney LLC (June 8, 2016)

- **SEC Findings Included the Following:** Morgan Stanley violated the Safeguards Rule because its policies and procedures were not reasonably designed to meet the requirements of the Safeguards Rule and failed to include:
  - Reasonably designed and operating authorization modules for the Portals that restricted employee access to only the confidential customer data to which such employees had a legitimate business need;
  - Auditing and/or testing of the effectiveness of such authorization modules; and
  - Monitoring and analysis of employee access to and use of the Portals.

What Will the SEC Really Want to Know in an Examination of Asset Managers, Investment Advisers, Custodian Banks, or Broker Dealers?

1. Do you truly understand your firm's cybersecurity infrastructure?

2. Have you enacted policies and internal procedures specifically tailored to your risks?

3. Can you prove - - with documents - - that you adhere to and enforce your own policies?

4. Can you detect - - in real time - - any unlawful access to your firm's data networks?

5. Are you actively monitoring and minimizing the risks associated with your third party vendors and service providers?

Thank You

For further information, visit our website at **dechert.com** or contact any of today's presenters.

Dechert LLP