FINRA/SIFMA Cybersecurity Conference

New York, NY February 4, 2015

Session 1: Establishing Cybersecurity Risk Management and Governance
Wednesday, February 4
10:10 – 11:00 a.m.

Speakers:

Karl Schimmeck (*moderator*)
Managing Director, Financial Services Operations
SIFMA

Zulfi Ahmed
Senior Vice President IT Risk/Global CISO
MetLife

Patrick Cox
Senior Vice President and Chief Privacy Officer
LPL Financial

Lisa Roth
President
Monahan & Roth, LLC

Biographies:

Karl Schimmeck is a Managing Director at SIFMA and is responsible, as staff advisor, for supporting SIFMA's work on cybersecurity, business resiliency, operational risk and technology risk. He serves on the executive committee of the Financial Services Sector Coordinating Council (FSSCC) and leads a number of sector initiatives related to third-party risk, exercises and information sharing. Prior to joining SIFMA, he held finance and operational risk positions at Goldman Sachs within Derivative Operations. Additionally, he's worked as a strategy consultant and program manager for a number of high-tech clients while working for PTC, and was also a Captain in the United States Marine Corps. He holds an MBA from the NYU Stern School of Business and a bachelor's degree in industrial engineering from Cornell University.

Ahmed Zulfi is Senior Vice President IT Risk, Global Chief Information Security Officer, MetLife. He is responsible for IT risk and security for MetLife globally. Working with senior management, he is responsible for evolving and executing MetLife's enterprise wide information security strategy, which protects MetLife and its customers' information, ensuring it is complying with applicable security related regulatory standards. In the Global CISO role, Mr. Ahmed oversees the creation and maintenance of information security policies and standards, risk assessments, security roadmap, incident response, DR processes, security controls, and security awareness and training programs. Mr. Ahmed is an accomplished IT executive with more than 25 years of professional experience in the IT, information security, and DR functions across multiple industries. He has worked for many notable corporations, such as PepsiCo, CVS/Caremark and Mobil/Exxon. He previously served as the Global CISO for PepsiCo for six years, CISO for CVS/Caremark for eight years, and has been recognized on numerous occasions for his work in the Information security industry. Most recently, he was recognized by ExecRank in the ninth position as one of the top IT security executives in the United States. Mr. Ahmed is also a member of the governing body for Evanta, a nationally recognized organization for CISOs, and has served as a speaker in the information security field. Mr. Ahmed has also written several articles in the Dallas Morning News. He has published several technical papers in the area of IBM UNIX operating systems.

Patrick Cox is Senior Vice President and Chief Privacy Officer at LPL Financial. He leads a group of professionals who manage infrastructure and vendor risk as well as privacy operations and incident investigations. Prior to joining LPL, Mr. Cox was Chief Counsel for The Personal Advisors Group and Chief Privacy Officer at Ameriprise Financial, and a Vice President and Senior Counsel at Morgan Stanley. Previously, Mr. Cox practiced law in New York, where he worked as a prosecutor in the Manhattan District Attorney's Office, as a law clerk at the U.S. Court of International Trade, and as an adjunct professor at Fordham University School of Law before entering private practice. He is a Certified Information Privacy Professional, a past chair of SIFMA's Privacy Subcommittee and Chair of the Financial Services Roundtable/BITS Operations and Technology Working Group. Mr. Cox graduated from Fordham University School of Law and Loyola Marymount University.

Lisa Roth is a registered principal with Keystone Capital Corporation; a FINRA member firm headquartered in San Diego, CA. Ms. Roth holds FINRA Series 4, 7, 24, 53 and 65 licenses. Ms. Roth is also the President of Monahan & Roth, LLC, a professional consulting firm offering regulatory compliance consulting, expert witness and litigation support services. Previously, Ms. Roth was the founder and CEO of ComplianceMAX Financial Corp., a regulatory compliance company offering technology and consulting services to more than 1,000 broker-dealers and investment advisers. Ms. Roth's leadership at CMAX led to the development of audit and compliance workflow technologies now in use by some of the United States largest (and smallest) broker-dealers and investment advisers. Ms. Roth has also served in various executive capacities with Royal Alliance Associates, First Affiliated Securities, and other brokerage and advisory firms. Ms. Roth has served on the FINRA Small Firm Advisory Board, including one year as its chair. She is the past chairman of the National Association of Independent Broker-Dealer (NAIBD), and has served on the Board of the Third Party Marketers' Association. Ms. Roth has recently completed a two-year term as a member of the PCAOB Standing Advisory Group. She is an active participant in industry forums, including FINRA committees and trade associations. Ms. Roth is a frequent speaker at industry and regulatory conferences, and serves on ad hoc committees as necessary to promote a culture of continuous improvement for compliance and operations among investment services firms. Ms. Roth resides in CA, but is a native of Pennsylvania, where she attained a bachelor's degree and was awarded the History Prize from Moravian College.

ONLINE RESOURCES CYBERSECURITY

Ten Cyber Security Tips for Small Business (FCC)
https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf

US SEC National Exam Program Risk Alert (OCIE Cyber Security Initiative)
http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf

2014 Verizon Data Breach Investigations Report
http://www.verizonenterprise.com/DBIR/2014/

FCC Cyber Security Policy Planning Guide Template
http://www.fcc.gov/cyberplanner

National Cyber Security Alliance – Mobile Tip Sheet (for personnel and customers)
http://staysafeonline.org/stay-safe-online/mobile-and-on-the-go/mobile-devices.

Cyber Security in the Golden State (see "Practical Steps")
https://oag.ca.gov/cybersecurity.

Boards of Directors, Corporate Governance and Cyber---Risks: Sharpening the Focus (a speech by SEC Commissioner Luis A. Aguilar)
http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VMviuMZh1B w

National Institute of Standards and Technology – Cyber Security Framework
http://www.nist.gov/cyberframework/index.cfm

National Institute of Standards and Technology – Cyber Security Roadmap
http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

OUTSOURCING DUE DILIGENCE FORM

SERVICE TO BE OUTSOURCED

1. **Type of service to be outsourced:**
   - ☐ Accounting/Finance: _____ ☐ Compliance Consulting: _____
   - ☐ Legal Services: _____ ☐ Administrative Functions: _____
   - ☐ Information Technology: _____ ☐ Operations/Support Functions: _____
   - ☐ Other: _____

2. Is this service essential to the operation of the Firm (i.e. transaction order entry; custody and prime brokerage; service designed to promote rapid recovery of operations etc.)? ☐ Yes ☐ No

APPROPRIATENESS OF OUTSOURCING

1. **Potential impact on Firm if service provider fails to perform:**

Financial Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Reputational Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Operational Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Customer Service Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Potential Losses to Customers:	☐ High	☐ Medium	☐ Low	☐ N/A
Comply with Regulatory Requirements:	☐ High	☐ Medium	☐ Low	☐ N/A
Costs to Firm:	☐ High	☐ Medium	☐ Low	☐ N/A
Degree of Difficulty Replacing Service Provider:	☐ High	☐ Medium	☐ Low	☐ N/A

Comments:

2. Is there an affiliation or other relationship between the Firm and the service provider? ☐ Yes ☐ No
   If yes, please describe the relationship and any potential conflicts of interest:

3. Is the service provider a regulated entity subject to independent supervision or jurisdiction? ☐ Yes ☐ No
   If yes, name of regulator: _____

SERVICE PROVIDER INFORMATION

1. **General Information**
   Vendor Name:
   _____

   Vendor Address:
   _____

   _____

   Contact Name(s): _____ CRD # (if applicable): _____
   Phone: _____ Fax: _____ Website: _____

2. Is the service provider owned/controlled by a Parent Co.? ☐ Yes ☐ No Name: _____

3. **Personnel:**
   Approximate # of employees:_____
   Does the service provider hire independent contractors? ☐ Yes ☐ No

4. **Background Information:**
   How many years has the service provider been in business? _____
   How many years has the service provider provided the outsourced function? _____

   Is the service provider known to the Firm or employees of the Firm? ☐ Yes ☐ No
   If yes, please name the individual(s) and describe any prior experience each had with the service provider:
   _____
   _____

DUE DILIGENCE

1. What methods did the Firm use to verify the service provider's information? (Choose all that apply.)

☐ FINRA Public Disclosure	☐ Internet Research	☐ Entity Formation Documents
☐ SEC Public Disclosure	☐ Credit/Background Check	☐ Independent Research
☐ Form BD/ADV	☐ Media/News Reports	☐ Personal Referral
☐ Business Plan	☐ 10K	☐ RFP
☐ Policies Manual(s)	☐ Personal Interviews	☐ Marketing Materials
☐ Financials	☐ Onsite Inspection	☐ Sales Materials
☐ Other:		

_____

Identify where this evidence is maintained of the above methods used to verify the service provider's information (i.e. copies of documents reviewed; notes from personal interviews and onsite inspections; printouts from public disclosure sites etc.)?

2. Please list one or more qualified references; firms that use this service (if contacted personally, identify the name of the contact and the result of the contact):

1.
2.
3.

3. Please describe the background and experience of individuals who will be performing the services:

4. Based on your review of reference and background information, has/have the service provider and/or its principals been subject to any regulatory, criminal or civil disciplinary issues? ☐ Yes ☐ No
   If yes, please describe:

5. Based on your review of reference and background information, please describe the service provider's ability and capacity to perform the outsourced activities effectively, reliably, and to a high standard (include in your description relevant technical, financial, human resources, and/or other assets of the service provider):

6. Confirm that the service provider has an adequate information security plan in effect. ☐ Yes ☐ No

   If yes, review a copy of the plan and comment on its adequacy including at minimum standards for compliance (NIST or other) and method(s) for breach reporting and mitigation:

7. Will the service provider have access to non-public information? ☐ Yes ☐ No

If yes, comment on the adequacy of the service provider's for safeguarding non-public information:

8. After reviewing the information, are there any questionable issues or potential conflicts of interest?
   ☐ Yes ☐ No
   If yes, please describe:

CONTRACTS AND AGREEMENTS

1. Has (or will) the Firm entered into a written agreement with the service provider? ☐ Yes ☐ No
   If yes, please identify the relevant provisions and disclosures in the contract (choose all that apply).

   ☐ Provides for Firm and regulator access to records
   ☐ Limitations on service provider's ability to sub-contract
   ☐ Defines responsibilities of all parties subject to contract
   ☐ Defines how responsibilities will be monitored
   ☐ Liability for unsatisfactory performance or other breach
   ☐ Requirement to maintain a disaster recovery plan
   ☐ Time Commitment (Termination Date):
   _____
   ☐ Other relevant provision(s):
   _____
   ☐ Firm and client confidentiality
   ☐ Payment arrangements
   ☐ Provide quality services measures
   ☐ Guarantees and indemnities
   ☐ Information security provisions
   ☐ Disclosure of breaches in security

2. Was the written agreement reviewed by the Firm's legal counsel? ☐ Yes ☐ No ☐ N/A
   If yes, name of legal counsel: _____
   Date of Review: _____

3. Was the written agreement reviewed by the principal responsible for outsourcing functions?
   ☐ Yes ☐ No
   If yes, name of principal: _____ Date of Review: _____

OVERSIGHT AND PERIODIC REVIEW

1. List the name and title of the Firm Principal who is responsible for the periodic oversight and review of the outsourced service? _____

2. Please identify the individual(s) who will monitor the outsourced service if different from above.
_____

3. Please identify the tools that will be used to monitor the outsourced service:

☐ Service delivery reports prepared internally
☐ Publicly available resources
☐ Internal auditor
☐ External auditor
☐ Other
☐ Service delivery reports supplied by the service provider
☐ Performance levels established in written agreement
☐ Onsite inspection
☐ Attestations by service provider

_____

4. Frequency of monitoring: ☐ Daily ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Annually
☐ Other
_____

5. If deficiencies are found, are there procedures in place to respond to such deficiencies (i.e. communicate with the service provider; terminate the contract)? ☐ Yes ☐ No

DOCUMENTATION REVIEW AND APPROVAL

1. Individual(s) responsible for completing this due diligence review:
   a. _____
   b. _____
   c. _____

Firm Principal: I have reviewed the information contained in this Outsourcing Due Diligence Form and:

☐ The Firm has elected to use the service provider above.

☐ The Firm will not use the service provider above.

_____ _____ _____
Principal Signature Date Printed Name of Principal

Electronic Devices and Communications Inspection Form

Electronic Device Review:

Device Name	Description	% Business Use	% Personal Use

□ Yes □ No Anti-malware software is installed on this device.

□ Yes □ No Anti-virus software is installed on this device.

□ Yes □ No Software auto-update is set to "ON" on this device.

□ Yes □ No Log in privileges to this device are password protected.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY approved (company) email is received on this device.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY associated personnel have access to this device.

Please explain any "NO" answer in the space provided below:

Exceptions, Notes:

Electronic Device Review:

Device Name	Description	% Business Use	% Personal Use

□ Yes □ No Anti-malware software is installed on this device.

□ Yes □ No Anti-virus software is installed on this device.

□ Yes □ No Software auto-update is set to "ON" on this device.

□ Yes □ No Log in privileges to this device are password protected.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY approved (company) email is received on this device.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY associated personnel have access to this device.

Please explain any "NO" answer in the space provided below:

Exceptions, Notes:

Cyber Security Incident Report

Complete the following form when any of the following events has occurred. Include incidents resulting from an accident or negligence, as well as those resulting from deliberate wrongdoing.

1. *Malware was detected on one or more Firm devices.*
2. *Access to a web site or network resource was blocked or impaired by a denial of service attack.*
3. *The availability of a critical web or network resource was impaired by a software or hardware malfunction.*
4. *An unauthorized user breached the network.*
5. *The compromise of a customer's or vendor's computer was used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a customer account or the submission of fraudulent payment requests purportedly on behalf of a vendor.*
6. *The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds of securities.*
7. *The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services.*
8. *An employee or other authorized user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information or damage to the Firm's network or data.*
9. *The Firm, either directly or as a result of an incident involving a vendor, experienced the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information.*
10. *Any other security breach event.*

Which of the above best describes the incident: (No.#): __

If (other) please describe:

Date detected: _____ Date Remediated: _____

How was the incident detected? ☐ Internally ☐ Externally ☐Not Known
What was the source of the incident? ☐ Internal ☐ External ☐Not Known
Please identify the cause of the incident. ☐ Deliberate wrongdoing ☐ Error, accident

Was client non-public data compromised? ☐ Yes ☐ No

Please describe the nature, duration, and consequences of the breach, how it was detected and how it was remediated:

Please provide any additional notes and/or details regarding this event, including the name(s) of any regulatory authorities to which the incident was reported.

Report Submitted by: _____ Date: _____

Report Reviewed by: _____ Date: _____

Bring Your Own Device ("BYOD")

Policy Development and Implementation Outline

- **Secure Mobile Devices**
  - **Authentication (passcode/PIN) requirements**
  - **Storage/transmission encryption requirements**
  - **Requirements to automatically wipe devices after a number of failed login attempts**
  - **Usage restrictions for mobile devices**
  - **Company rights to monitor, manage and wipe**
    Invest in a mobile device management (MDM) solution to enforce policies and monitor usage and access.
  - **Enforce industry standard security policies as a minimum: whole-device encryption, PIN code, failed login attempt actions, remotely wiping, etc.**
  - **Set a security baseline: certify hardware/operating systems for enterprise use using this baseline.**
  - **Differentiate trusted and untrusted devise access: layer infrastructure accordingly.**
  - **Introduce more stringent authentication and access controls for critical business apps.**
  - **Add mobile device risk to the organization's awareness program.**

- **Address App Risk**
  - **Use mobile anti-virus programs to protect company- issued and BYOD malware-prone mobile operating systems with mobile anti-virus.**
  - **Ensure security processes cover mobile app development and leverage tools, and vendors to bridge assessment skill gaps.**
  - **Manage apps through a mobile app management product.**
  - **Introduce services that enable data sharing between BYOD devices.**
  - **To increase productivity and security, continually assess the need for new apps.**

- **Manage the Mobile Environment**
  - **Create and enforce an appropriate BYOD support and usage policy.**
  - **Revamp support provisioning and de-provisioning (wipe) of devices, and an increased level of self-help.**
  - **Create a patch education process to encourage users to update their mobile devices.**
  - **Introduce a social support mechanism to augment the existing IT support team.**
  - **Implement a wiki/knowledge base employee self-service support solution.**

- **Test and Verify the Security of the Implementation**
  - **Perform security testing and review of the implemented solution**
  - **Use an integrated testing approach combining automated tools**
  - **Perform manual penetration testing**

- **Test Infrastructural Changes Affecting Mobile Connections to the Enterprise Network**
  - **Wi-Fi deployments**
  - **VPN endpoints**