

Customer Journey Analysis: Securing Social Media Strategy in the Financial Industry

Published: February 2016

Report Number: A0197

Analyst(s): David Houlihan, Esq., Principal Analyst

Share This Report



What You Need To Know

The maturation of social media has created a significant expansion in channels for internal collaboration and external market engagement. The openness and speed of communication available through enterprise social media also creates attendant security, reputational, and legal and compliance exposures. For the financial sector, in particular, stringent regulation, high likelihood of cyber-crime targeting, and the complexity of partner environments create a high probability of incidents and stakes that have traditionally served to discourage adoption.

As customer expectations on communication channels continue to change, the benefits of social strategies become increasingly attractive. These factors result in a need for clear roadmaps defining how financial institutions balance compliance and risk management requirements with the upside presented by social media strategies in ways that minimize the demands placed on limited organizational resources. In an effort to provide guidance through these challenges, this report draws from in-depth research interviews with participating financial services firms to summarize key elements of the customer journey taken to develop risk-sensitive and compliance strategies to enable enterprise social media strategies.

Business Drivers: Social Media Strategy Enablement

The expansion of social media has brought new methods of engaging with customers and key stakeholders with increasing importance to the scope and value of client engagement strategies. As these channels mature and gain mainstream market saturation, they take on increasingly greater importance as business development and internal collaboration tools. This is particularly true in the marketing

AT A GLANCE

Social Media Strategy Objectives

- Increased product / services awareness
- Improved brand awareness and value
- Increased support for and control over agent and advisory messaging
- Enhanced internal collaboration

Obstacles to Strategy Adoption

- Scope, variety, and severity of risk associated with social media use
- Difficulty providing adequate monitoring and management of social media channel volumes with existing compliance resources

Key Strategy Components

- Legal and compliance drives strategy
- Multi-stakeholder planning committees involving marketing, compliance, and risk
- Strategy development follows channel use, access, needs, and business risk assessment
- Policy defined according to organizational priorities, risks, and user incentives
- Social strategy rolled out by phases according to value with attendant training and awareness programs
- Program supported by automated channel monitoring and controls management tools

Research Participant Demographics

Research analysis focuses on business drivers, policy development, change management, and support technology adopted by two U.S.-based financial services organizations demonstrating successful adoption of social media strategy.

- Revenue: \$1 billion to \$3 billion
- Employee Headcount: 2,500 to 11,000

communications world as old direct marketing strategies have given way to digital, multi-touch, multi-channel, and customer experience-oriented strategies.

Blue Hill research interviews with participants largely echo these trends, with participants characterizing their firms as “traditional” organizations, reluctant to adopt social media strategies. However, both organizations indicated increased pressure to develop social media strategies as they found they were beginning to lose business and mindshare to competitors with more liberal social media policies and active social channel engagement. In addition, the participants identified a high degree of internal interest in adoption from marketing and sales departments. To this end, the key constituencies pressuring for strategy expansion reported were: marketing, sales, and third-party associates. Participants identified the third group as contributing particularly strong incentives to change due to increasing “rogue” use of social media channels to engage with prospects. Similarly, the organizations found that despite policy bans or constraints, the solutions were widely used within the organization.

Factoring the risks presented by eroding market opportunity and lack of visibility, the organizations began to develop their own social media strategies. In spite of traditional reluctance, the participants demonstrated a sophisticated and diverse set of objectives for their strategies (Table 1).

Table 1: Objectives of Enterprise Social Media Strategy

	Factor	Objective	Value Indicators
Marketing Strategy	Awareness	Increase market awareness and promotion of products and services	<ul style="list-style-type: none"> • Number of direct impressions created through social channels • Number of new inquiries achieved through social channels
	Brand	Enhance corporate brand awareness and associated value	<ul style="list-style-type: none"> • Number of indirect impressions created through third-party discourse in social channels • Percentage of customer mentions with “positive” sentiment
	Customer Support	Demonstrate expertise and value through shared “tips and tricks”	<ul style="list-style-type: none"> • Prospect conversion rate • Customer retention rate • Net promoter score
Associate Support	Engagement	Enhance partner engagement and success rate with prospects	<ul style="list-style-type: none"> • Revenue generated through partner channels
	Risk	Maintain visibility and control over brand and associate representations	<ul style="list-style-type: none"> • Number of unapproved representations or messages sent by partner under corporate brand • Imposed liability derived from partner activities
Internal Collaboration	Collaboration	Remove data and process silos between related functions	<ul style="list-style-type: none"> • Time lost to delays in stakeholder feedback / response • Quality and accuracy of work product and decision making

Source: Blue Hill Research, February 2016

Risks and Obstacles to Social Media Strategy Adoption

The profiled organizations reported a set of obstacles and risks in the implementation of social media strategy as diverse and varied as their business objectives for the programs (Table 2). The priorities reported by participants lay with increased cyber-threats, particularly through hijacked or spoofed accounts that could impact customer relationships as well as the complex set of controlling regulations. An [analysis of social media activity among Fortune 100 companies by Proofpoint Nexgate](#) indicates that financial services firms face the greatest exposure, encountering 250 social media compliance risk incidents a year, *3.6 times as many incidents* as the average Fortune 100 organization analyzed. Financial services organizations face greater exposure because they operate at the intersection of stringent industry regulations and highly motivated bad actors.

The underlying challenge reported by participants did not rest with the risk itself, but the operational challenges presented by social media channels in monitoring and managing those risks. The ability to address risks presented by social media use requires that organizations identify risk generating content and scenarios. The volume, variety, and democratization of use created by social media channels creates a tremendous barrier to an organization's ability to make those identifications.

“

Our associates go where their buyers are. That means we started seeing them posting corporate-branded content on Pinterest or Instagram. They are doing the right thing; they are going where the customers are. They know the next thing. The problem is: compliance knows the last thing, so there's no line of defense. We had no controls, no guidelines, and poor awareness of the channels.

”

*Associate General Counsel
Financial Services Firm*

Table 2: Risks Presented by Social Media Enterprise Social Media Strategy

	Risk	Challenge	Exposure
Compliance	Disclosure	Regulatory controls on method / content of “material impact” statements	<ul style="list-style-type: none"> Fines and sanctions imposed by regulatory agencies Cost of legal, compliance, and executive engagement in resolution
	Discourse	Regulatory controls on permissible advertising or representations	<ul style="list-style-type: none"> Fines and sanctions imposed by regulatory agencies Cost of legal, compliance, and executive engagement in resolution
	Management	Regulator controls on control / inquiry into customer accounts	<ul style="list-style-type: none"> Fines and sanctions imposed by regulatory agencies Cost of legal, compliance, and executive engagement in resolution
Reputation	Disclosure	Shareholder and customer response to content of representations	<ul style="list-style-type: none"> Loss of share value Lost business opportunities Erosion of brand value and goodwill
	Discourse	Shareholder and customer response to tone, language, opinions expressed	<ul style="list-style-type: none"> Loss of share value Lost business opportunities Erosion of brand value and goodwill

	Risk	Challenge	Exposure
Cyber-threat	Data Breach	Unauthorized data access by third-parties for criminal or customer exploitative uses	<ul style="list-style-type: none"> Competitive consequences of corporate data release Legal and regulatory exposure related to exposure of customer data Reputational harm derived from breach and/or exposed content Cost of remediation, investigation, and audit related to breach
	Hijacking	Unauthorized access and use of corporate accounts by third-parties	<ul style="list-style-type: none"> Reputational harm derived from unauthorized account use Legal and regulatory exposure related to unauthorized account use Cost of remediation, investigation, and audit related to breach
	Fraud	Use of false accounts to spoof corporate accounts or to obtain access to corporate stakeholders	<ul style="list-style-type: none"> Exposure to blackmail or information loss to third-parties Reputational harm derived from falsified account use Legal and regulatory exposure related to unauthorized account use Cost of remediation, investigation, and audit related to breach

Source: Blue Hill Research, February 2016

To provide a sense of the scope of effort involved, consider [the Proofpoint Nexgate analysis](#), which indicates that the average Fortune 100 company faces 70 compliance risks and 19,000 content risks out of 38,191 brand posts and 546,658 commenter posts. As such, only approximately 3.26% of the content that must be reviewed by the organization represents potential issues of investigation. The challenge lies in locating these posts in a timely manner without taxing corporate compliance resources.

While not operating on the same scale, the profiled organizations reported the same issue: an impasse created by the need to permit stakeholders to engage with social media with speed and flexibility without the human resources needed to monitor, manage, and address risks as they occur.

Estimating the ROI of Social Media Risk Prevention Investments

A top financial institution was able to reallocate **\$158,000** in personnel costs to business-critical functions by switching to automated moderation. Read Blue Hill's [Estimating the ROI of Social Media Risk Prevention Investments](#) for more information on calculating the value of social media security solutions.

Components of Risk-Aware Social Media Strategy Development

Executing on the goals reported by the participants for their social media strategy required a balance of flexibility and control to simultaneously mitigate risk and minimize bottlenecks present by and operational burdens placed on compliance and monitoring personnel. Achieving this balance requires careful planning and policy development, coordination of cross-functional stakeholders, and effective use of supporting technology. Research participants demonstrated a strong combination of these factors, demonstrating standout characteristics in (1) stakeholder engagement, (2) needs analysis, (3) policy development, (4) strategy execution and oversight, and (5) supporting technology adoption. Table 3 summarizes these factors as reported to Blue Hill Research.

Table 3: Components of Adoption of Social Media Risk Management and Protection Transformation

	Steps Taken
Stakeholder Engagement	Compliance and legal departments lead strategy development and program monitoring
	Planning committee involved representatives from senior management, marketing, human resources, information security, social media communications, compliance, and legal
Needs Analysis	Review and prioritization of identifiable existing exposure
	Assessment of channels / content types presenting highest Value at Risk
	Survey of perceived channel needs and required use by stakeholders
Policy Development	Identification of business needs and incentives for stakeholder compliance
	Policy framework developed from FINRA social media guidelines, SEC guidance, client feedback, and investment advisor requests
	Articulation of acceptable limitations on stakeholder use and disclosure
	Definition of Code of Conduct, acceptable use policies, and oversight methodology
Strategy Execution & Oversight	Phase-based rollout of social strategy prioritizing identified “high activity” users
	Launch of comprehensive training and awareness programs
	Daily content meetings involving corporate communications, marketing, and compliance
	Continuous improvement adjustments based on user feedback and observed risk exposure
Technology Stack	Automated channel monitoring solution
	Automated access control and policy solution

Source: Blue Hill Research, February 2016

Key Observations and Takeaways

As the core components of the profiled organizations risk mitigation and compliance management efforts, the factors identified in Table 3 represent fundamental enablers of the organizations ability to engage in social media strategies. Individualized analysis of these factors falls outside of the scope of this paper. However, several key themes emerge across these characteristics:

- 1) Cross-functional coordination on needs assessment, policy development, and ongoing oversight
- 2) Combination of internal needs and use cases with regulatory guidelines and client feedback
- 3) Prioritization of “high activity” users to maximize strategy benefits and risk awareness
- 4) Deployment of automated monitoring and controls management solutions

The fourth theme deserves particular attention for the role it plays in addressing the key challenge identified above: *the balance of risk mitigation with minimal oversight labor burdens for compliance and minimal delay and limitation for social media users*. To this end, the profiled organizations demonstrated a use of automation in both content monitoring and access control and policy management. These capabilities represent two components of an emerging social media protection technology stack intended to help organizations keep pace with the expanded oversight challenges contributed by social media channels. Key functionality includes:

- **Channel Monitoring:** automated review of social content for risk indicators and policy violation
- **Automated Controls:** rules-based management of account access, permissions, and behavior
- **Compliance Workflow Management:** automated management and progression of processes related to review and incident management following discovery of high risk data or exposure

This suite largely parallels the automation and monitoring stack supporting marketing strategy execution, but with a specialized focus on mitigating the mix of regulatory, legal, and security exposures posed by social media use. The profiled organizations identified this stack as a key enabler to the ability to execute risk-sensitive social media strategies by removing human effort required in content review. Rather the solutions permitted the organizations to limit review efforts on the limited pool of content that had been machine identified as presenting potential risk. In this way, these solutions contribute net reductions to compliance time burdens as well as the occurrence of risk incidents. Organizations seeking to understand more about these tradeoffs and methods for estimating the net impact to organization value are advised to review Blue Hill's [Estimating the ROI of Social Media Risk Prevention Investments](#) Analyst Insight.

“

We need to be able to capture the biggest picture of what's out there and what might affect us, not just what four reviewers might find. We need to have eyes on our feeds 24/7. Our tool gives us those eyes while we sleep and helps us narrow in on the risk items. We start with the hits that the solution identified and let our human reviewers start there. It streamlines the process and helps escalate the issues that we need to worry about.”

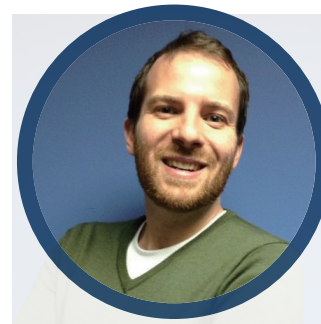
*Associate General Counsel
Financial Services Firm*

ABOUT THE AUTHOR

David Houlihan

Principal Analyst

David Houlihan researches enterprise risk management, compliance and policy management, and legal technology. He is an experienced advisor in legal and technology fields with a unique understanding of complex information environments and business legal needs.



CONNECT ON SOCIAL MEDIA



@DWHoulihan



www.linkedin.com/in/houlihandavid



bluehillresearch.com/author/david-houlihan/

For further information or questions, please contact us:

Phone: +1 (617)624-3600

Fax : +1 (617)367-4210

Twitter: @BlueHillBoston

LinkedIn: www.linkedin.com/company/blue-hill-research

Contact Research: research@bluehillresearch.com

Blue Hill Research is the only industry analyst firm with a success-based methodology. Based on the Path to Success, Blue Hill Research provides unique and differentiated guidance to translate corporate technology investments into success for the three key stakeholders: the technologist, the financial buyer, and the line of business executive.

Unless otherwise noted, the contents of this publication are copyrighted by Blue Hill Research and may not be hosted, archived, transmitted or reproduced, in any form or by any means without prior permission from Blue Hill Research.