conversocial

Executive Summary:

Compliance and Social Customer Service

Financial Compliance in Social Media

Financial institutions, banks, brokers and insurance companies, often have a wide number of compliance obligations to meet when undertaking activities on social media, and this can frequently lead to more significant challenges to social media adoption than encountered in other sectors. While many financial sector regulators have published best practice guidance on use of social media, requirement of controls around supervision, content, recordkeeping and governance, these frequently focus on professional networking and marketing purposes, where static financial messages may be promoted through social media.

Here we describe some of the key issues to be considered when embarking on a customer service strategy on social media, involving dynamic and individual messages to individual customers, and additionally how the Conversocial product is built to assist financial services companies in meeting their compliance requirements.

95% of all customer interactions in retail banking will be digital by 2020

- CameoWorks

Benefits of a "Social First" Approach

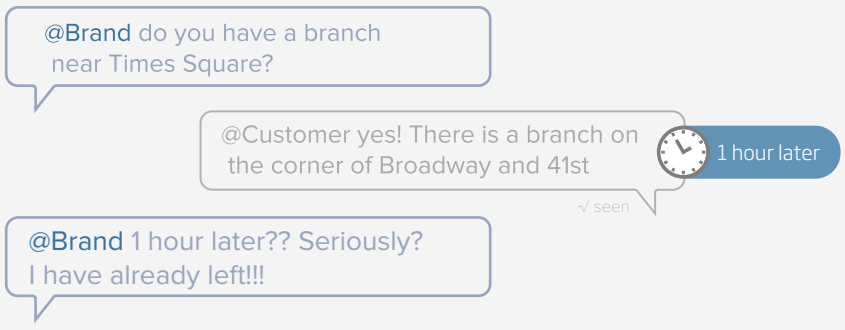
Financial services companies are increasingly adopting new social media strategies to optimize customer response times and enable flexible and high quality customer service across a broad range of mobile channels. Using social for customer services enables financial services customers to humanize and individualize the experience for each customer and more importantly increase customer engagement and satisfaction. This is critically important for customers looking to engage with younger more tech savvy consumers that rely heavily on social media who wish to communicate with their providers through social channels.

Balancing Responsiveness and Compliance: Best Practices for Financial Services

In adopting social strategies, financial services customers inevitably have a greater need to balance compliance needs with social responsiveness and high quality customer services. With this in mind, a number of best practices for operating on social media should be considered, particularly in the context of the guidelines by regulatory bodies such as the SEC and FINRA in the US, the FCA in the UK, and the IIROC in Canada.

While extensive commentaries have been published on social media usage in financial services, and helpful guidelines are widely available, these frequently focus on managing static content and potential promotional communications, to minimize misleading advertisements to the public.

The purpose of this white paper is to summarize some of the key considerations and describe how Conversocial enables you to provide customer service on social media in a responsive but compliant manner.



66% of consumers expect a response on Social Media within an hour. 56% of consumers want a response within 30 minutes - Ovum

Supervision

From a risk and compliance perspective, financial services companies need to ensure that all communications with customers, through any channel, social or otherwise, are appropriately supervised. Obvious best practices we have seen include: creating clear escalation pathways for any serious issues, and more importantly, creating clear rules to evaluate matters for which customers should be taken off social (i.e., to minimize for instance non-compliance with privacy, data protection or PCI compliance issues). This involves consideration about which channels are most appropriate to connect with individual customers to resolve issues as expeditiously and securely as possible.

A standard escalation pathway may typically involve:

a) Initially taking the social user to a private channel such as Facebook Messenger (which is encrypted both in transit and at rest) for first line authentication - this may simply involve verifying a phone number, name and address against internal records;

b) Subsequently sending the social customer to a secure site within your required resolution SLA. This escalation may include to web chat, SMS, phone or other secure authorized private channel.

It is noteworthy that turning to a new communication channel (rather than a pre-approved escalation path) for financial services customers is not easy - especially from a compliance perspective - where transmission of personal information may be required.

The strategy a financial services firm adopts will depend on the resourcing and sensitivity of communications - and ultimately, from a risk perspective, many financial firms are likely to move to their preferred secure channel at some higher escalation point - as this minimizes any transmission of sensitive personal information to outside vendors.

Content Approval

While general dynamic social customer service dialogue may not typically require specific pre-approval in the same way that static content and advertisements do, it is nevertheless necessary to monitor communications and, where necessary revisit and review such communications. Additionally, financial services companies may wish to consider using generic templates and pre-approved standard material to assist in managing content and optimize response times in a way that reduces the risk of non-compliance.

Financial customers are left striking a delicate balance between managing/controlling communications that could be considered financial promotions (under FSMA for instance), ensuring they are being “fair, consistent and not misleading” and at the same time avoiding to act like robots on social media. Clear rules and controls enable customers to humanize the experience of their customers and avoid acting like “robots”. We have found that content pre-approval in the social customer service environment may not strictly be necessary, provided clear rules are in place to minimize the likelihood of exchange of personal information through public social channels. That said, it is certainly prudent to have documented social media procedures, policies and process available (and distributed) on a company intranet to optimize social teams’ compliance with internal rules and policies.

68% of global financial customers yet to use mobile financial services due to concerns over security, usability, and service ubiquity.

- Inside the world of mobile financial services, What people want, Ovum-Amdocs

Staff Training

Ensure comprehensive staff training on social media usage and that documented policies are approved, circulated and enforced. Employees should have a clear understanding what they should and should not post to social platforms and how they should handle any specific customer posts.

Even though it is clearly best practice to limit personal information communicated publicly on social channels, it is surprising how many users may either unintentionally, or otherwise, in fact post their email address, phone number and other details publicly. Training should include how to limit the likelihood of this arising, and also managing this when a user does in fact publish any personal information on social media. Your social media partner will enable you to review communications systematically as part of a general audit plan and periodically scrub such data. Any employee breaches of policy should be followed up and dealt with.

Ultimately, the key focus of any effective customer service strategy is managing compliance requirements and optimizing responsiveness. Indeed, in the UK specifically, the FCA has set specific time frame requirements for handling complaints.

This makes social media a critical aspect of any customer services strategy. Using Conversocial, this can be achieved in a controlled and compliant manner. Some of the specific Conversocial controls are highlighted below.

28.7% of financial institution executives say managing compliance is their greatest challenge in 2016

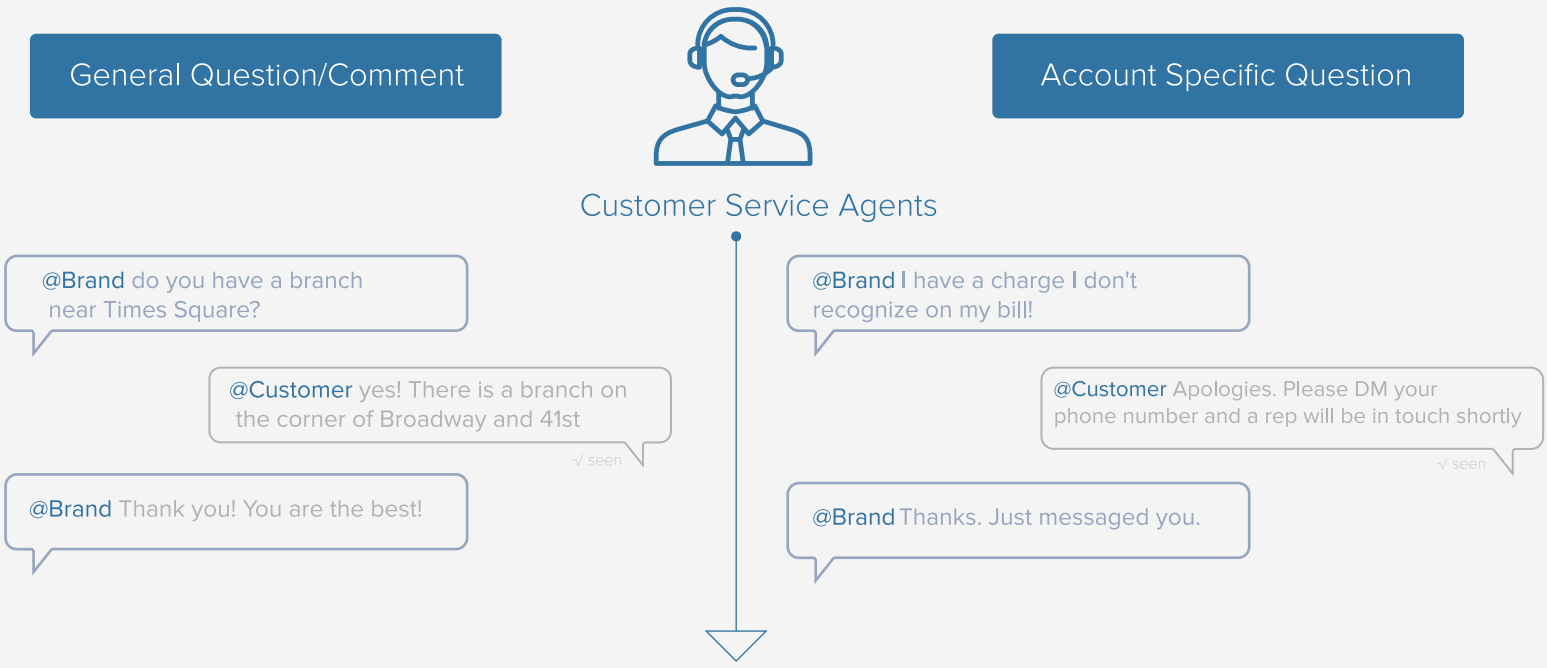
- Computer Services Inc. (CSI), "Executive Report: 2016 Banking Priorities Study," Jan 19 2016.

Record Keeping:

A critical issue for financial services companies is the ability to ensure that all records of customer interactions are not only controlled and retained, but also appropriately retained and searchable in an accessible place. Ensure your preferred social provider can enable you to retain all records to enable full record retrieval external of the platform itself. Different sectors have different data retention obligations, and the customer will need to ensure that their social media partner can comply with such requirements. For instance under FINRA rule 3110 a firm must retain the data for 3 years. Analogous requirements under the FCA, SEC and other regulations apply to other financial services companies.

Does the social platform meet the minimum best practice requirements?

- ☑ Encryption of data in transit and at rest?
- ☑ 3rd party penetration tests for security?
- ☑ Archived history of all conversations?
- ☑ Training, Approval, and Supervision workflow?



☑ Customer Resolution

Conversocial Security Controls

The controls that Conversocial enables to support financial services compliance are described below.

Third Party Attestations:

Conversocial's platform and processes undergo third party audits and international standard attestations to ensure compliance with information security practices. These include ISO27001, the international standard for information security management and third party network penetration testing. ISO27001 is an internationally recognized management system that maps controls broadly to a wide range of other industry accepted security standards including PCI DSS and SOC 1/2. It is also closely aligned to the SEC OCIE cyber security controls and has been referenced as an industry standard benchmark by the FCA. Conversocial provides its most recent audit results on request under NDA. Additionally, Conversocial's hosted data center has a wide array of third party compliance certifications and attestations including: SOC 1,2,3; ISO27001; ISO27018; and others. Please email security@conversocial.com for more information.

Encryption:

Conversocial uses EBS volumes to encrypt at rest (AES-256) in line with NIST Special Publication 800-38E. Conversocial encrypts data in transit (SSL) through the use of ECDSA which is designed to maintain the integrity of financial messages (See Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

Archival/Data Retention/Reporting:

For financial services clients who need to comply with specific data retention requirements, Conversocial enables the customer to export and store a searchable record trail of their data on the system. All data can be archived, exported and retained and/or deleted in line with customer's data deletion practices and retention obligations. Conversocial enables access to an export API to plug into customer's existing in-house or third party archive system and provide date stamped content for archival purposes.

conversocial

Archival/Data Retention/Reporting:

For financial services clients who need to comply with specific data retention requirements, Conversocial enables the customer to export and store a searchable record trail of their data on the system. All data can be archived, exported and retained and/or deleted in line with customer's data deletion practices and retention obligations. Conversocial enables access to an export API to plug into customer's existing in-house or third party archive system and provide date stamped content for archival purposes.

Rules:

Financial services customers can set bespoke social media rules and monitor social media content to ensure compliance. For instance, this can enable customers to create rules that require user-level approval before a social media post is released. Additionally, large multinationals can set multiple rules across different jurisdictional teams, depending on the location of the team. Financial services customer may also wish to create standardized and approved content libraries to control outgoing content which does not require such approval. This enables customers to optimize response times and ensure they are providing the best customer service experience.

Conversocial Security Controls

The controls that Conversocial enables to support financial services compliance are described below.

Fine-grained Access and Password Controls:

It is important for customers to manage passwords in line with their internal password requirements. Conversocial enables clients to highly customize password requirements and align these to business needs with customizable role-based permissions. Such customization additionally includes an ability to set their own password policies; time-out requirements; rules of least privilege; and assignment of unique user IDs. Additionally, Conversocial enables IP white listing to control who can access content and restrict access to specific locations. It restricts access to a machine, group of machines or specific office location.

Governance:

Conversocial enables financial services to closely manage, audit and control all content being sent and received through social channels. Granular enterprise grade access controls and permissions, including admin oversight enable financial services customers to restrict access and enables a fully auditable trail of agents' response. Conversocial provides comprehensive onboarding and training of the platform features and controls and our customer success team has assisted with a number of installations for highly regulated customers and can provide helpful tips and guidance during implementation.

See a recent case study by one of our financial sector customers below.

Read BMO Case Study

Or email socialfirst@conversocial.com