Risk Report on Electronic Communications

for the Financial Services Industry in Europe
Contents

Executive Summary .................................................. 3
Key Areas of Risk Posed by Electronic ......................... 5
Communications
Appendix 1 ............................................................. 11
Executive Summary

The last decade has seen a change in the attitudes of governments and regulators toward the financial services sector. With increased regulatory requirements and a tougher stance from regulators on enforcement, financial services organisations need to re-examine the risks posed by communications sent by employees both internally and to the public.

There is increased risk in this area as new channels of real-time communication are adopted within financial services organisations to facilitate communications and collaboration. These real-time communication channels expose organisations to non-compliance with regulatory requirements, data leakage, and litigation.

This whitepaper examines these risks and provides eight recommendations for financial services organisations to reduce their exposure to those risks.

Mapping the Regulatory Landscape

The financial crisis that swept through major financial centres throughout the world is still being felt by many economies in Europe today. That financial crisis and the reasons behind it have led to a change in regulatory attitudes toward the financial services industry in Europe.

Over the last five years regulators across the world have introduced or updated guidelines around the use of electronic communications within financial organisations. As a result, regulators across Europe and in the U.S. have shown less tolerance towards those who have not complied with regulations. For instance, U.S. financial services regulator, Financial Industry Regulatory Authority (FINRA), doled out more than US$15 million in fines against 66 electronic communication cases in 2013. Although the increase in the number of cases was small – only a 5% increase from the previous year’s 63 cases – the fines have more than doubled.

Accelerating Use of Electronic Communications

Another driver for tighter regulations around electronic communications is down to the commonplace use of multiple real-time communication channels within the workplace. Now, workplace communications do not just take place over email, they also take place on instant messaging systems, unified communication platforms (i.e. collaboration tools like Sharepoint as well as voice and video), and enterprise social networks. In a study conducted by Osterman Research, corporate users spent an average of 30 minutes on a typical workday using either a standalone instant messaging system or one which is integrated with a collaboration tool.\(^1\)

In fact, industry analyst, Gartner, predicts that by “2014 social networking services will replace e-mail as the primary vehicle for interpersonal communications for 20 percent of business users.”\(^2\) And this prediction is already coming true. In 2015, it was reported that employees of

---


one of the largest Swiss banks will send more instant messages than emails for the first time. Email will account for just 48% of the total communications sent by its employees.

Adoption of collaboration and social networking tools in the enterprise is also growing. 93% of marketers now use social media for business. Other functions within the organisation are also adopting social media. Human resources use it for recruitment and to research new hires. And financial services organisations have started to provide vital and personal rapid response customer services on Twitter.

However, electronic communications is an area of constant innovation with new technologies being launched all the time. For instance, a number of financial services organisations have joined forces to launch a new instant messaging platform called Symphony, which looks set to disrupt the dominance of established secure messaging services in the market.

As the use of this multitude of electronic communication channels becomes mainstream within any organisation, it exposes the highly regulated financial services organisation to new areas of risk.

Rise in Disciplinary and Precautionary Actions

An increasing number of businesses have taken disciplinary action against an employee for misusing social media. A recently published survey says this number has doubled over the last two years since the survey was conducted, and is an issue that currently faces 70% of firms.
This is clearly a growing area of concern for organisations and one which organisations need to take steps to address.

**Key Areas of Risk Posed by Electronic Communications**

Unauthorised activities such as harassment, discrimination, unfair competition, and defamation can now take place over electronic communications and are presenting new areas of risk that organisations need to be aware of, monitor and address. If left unchecked, these issues can be damaging to a firm, with consequences ranging from litigation, costly settlements, and negative publicity.

1. **Harassment**

Electronic communications open up a flood of potential avenues for harassment. As messages are sent via instant messaging systems, social networks, and others, which are often used for personal communications, users may not realise that harassment via electronic communications is treated in the same fashion as an in-person joke, inappropriate comments, or conduct. Employers have to ensure that all their electronic communications networks are not being used to create an intimidating, offensive, or hostile work environment for their employees.
2. **Discrimination**

An employer’s actions are governed by the same anti-discrimination laws and standards applied to all forms of communication, whether that action is in-person, on the phone or over email or a social network. What this means is that employers need to apply policies consistently from employee-to-employee when imposing discipline. Communications, even those sent internally within the organisation cannot discriminate against any protected characteristic, including race, gender, age, national origin, disability, and sexual orientation.

3. **Misuse of company confidential information**

Electronic communications can provide avenues for employees to woo customers from ex-employers which could violate termination or confidentiality agreements.

There are also more opportunities for company confidential information to be inadvertently or maliciously shared by employees. Instances of data leakage include customer information or a company’s financial results. For the financial services industry, this has implications on two levels. The industry relies on consumer trust in the brand. The leakage of customer confidential information could have devastating consequences on the business. Industry regulations also stipulate that the organisation could be held liable for statements or inaccuracies reported or leaked on social networking sites.

4. **Defamation**

There are serious consequences for those spreading false rumours, or making disparaging comments whether they are about colleagues or others outside of the organisation. The consequences are the same whether those comments are made in person or sent via instant message or social media. If they are proven to be untrue, recent case law in the U.K. (Lord McAlpine v Sarah Bercow) demonstrates that there is no ‘safety in numbers’—even forwarding or re-tweeting defamatory comments can lead to exposure to possible libel action.

5. **Misrepresenting View of Company**

High profile cases have highlighted how easy it is for slip-ups to happen on electronic communication platforms that can damage brand equity and generate negative publicity for any company. The speed by which communications can go ‘viral’ on real-time electronic communication channels amplifies even the most innocent of mistakes and very quickly turns it into headline grabbing news.
Take the case of an employee from a well-known supermarket chain in the U.K. who put up a poster meant for the staff room in the shop window. The poster was meant to motivate staff to encourage customers ‘Spend an extra 50p’ at every shopping trip, and encouraging staff to think about how that small amount could make a vast difference to the takings of the store. A passer-by spotted this poster in the window of the store, took a photo on his camera phone and shared it on Twitter. Within hours, it was re-tweeted thousands of times, and picked up by major news outlets. The result was an embarrassing public relations episode for the supermarket chain.

6. Unsanctioned Conduct

The manipulation of LIBOR and Forex rates has put electronic communications, and how they are used within financial services, firmly back in the spotlight. Instant messaging systems were used by traders to collude with their benchmark setting colleagues in the case of LIBOR. While currency traders from separate institutions were found to have used private chat rooms to facilitate their discussions to rig foreign exchange rates.

In both instances, the financial institutions involved have faced fines in the billions of pounds. The full impact of these two scandals is yet unknown, as the justice systems in Europe and U.S. are still in the process of bringing criminal cases through the judicial process. However, what these cases have highlighted is the need to bring electronic communications used within organisations under control.

7. Non-compliance with Regulations

Regulations that govern the use of electronic communications within the financial services industry already exist. And, in recent years, new regulations and guidelines have been issued to clarify the use of newer forms of electronic communication such as social media.

The Financial Conduct Authority (FCA) in the U.K. had previously issued a Policy Statement in March 2008 (as the Financial Services Authority) with a definition of the sorts of communication channels that fall into the category of electronic communications:

“It includes fax, email, Bloomberg mail, video conferencing, SMS, business to business devices, chat and instant messaging. But is not limited to these as it captures any electronic communications involving receiving client orders and the agreeing and arranging transactions. We will not produce an exhaustive list of electronic communication because..."
of the continuing innovation and advancement in technology which would mean the list frequently becomes out of date. We also feel that it is inappropriate to limit the obligations to a prescriptive list and an outcome based approach is more suitable in implementing such rules. We would expect senior management to exercise their judgement in this area.”

The regulations around the use of electronic communications fall into one of the following categories – record retention, supervision, and communications with the public. A list of regulations applicable to electronic communications issued by regulators in the U.K. and E.U. can be found in Appendix 1.

**Mitigating Risk – 8 Point Action Plan**

Within financial services institutions there are probably multiple communication channels in use, some could be deployed by corporate IT, such as the Bloomberg terminals, and others could simply be publicly available, such as Twitter and Facebook. While electronic communications can break down the barriers to communication and collaboration within the firm, and can facilitate marketing to prospects and customers, they could also pose threats to the organisation if appropriate action is not taken to mitigate the risks.

Here are 8 steps that organisations can take to mitigate the risk of electronic communications today:

1. **Establish an Active Compliance and Monitoring Programme to Review Content.** Technology exists that enables firms to monitor and block messages from being sent based on keywords or key phrases. An automated alert would then be sent to the supervisor or Compliance to review the message before deciding whether it can be sent.

2. **Notice of Ongoing Monitoring.** Employees should be notified that their communications are being monitored and retained as appropriate. These messages and other disclaimers can be appended to outgoing messages as a reminder and a deterrent.

3. **Employee Training.** This means providing employees with examples of best practices, and also highlighting instances that would not be acceptable usage of the electronic communications platform. It would also be a good idea to repeat the training on a regular basis (for instance, every year) to reinforce and remind employees of the expected behavior.

4. **Clearly Written Policies on Appropriate Use.** These should be kept up to date and distributed to employees. Copies should be kept in an accessible place for employees to reference. These need not be created from scratch – many regulated firms adapt their existing email policies to encompass other forms of electronic communications.
5. **Explicit Provisions on Misuse for Departing Employees.** Employees need to be made aware that they could be disciplined, dismissed, and even reported to the regulator if they misuse electronic communications. This should be clearly outlined and communicated to employees when they begin their employment.

6. **Insider Risk Awareness and Detection Programme.** Firms may want to set up a confidential hotline or email that allows employees to report any suspicious behavior to Compliance and Ethics Committees.

7. **Archiving and Defensible Disposition Policies.** Good record retention policies are not only essential for compliance with regulatory requirements, but also necessary to demonstrate chain of custody for evidence submitted in court cases. With an increasing number of court cases citing electronic communications other than email as evidence, firms need to put in place systems and processes to establish legal hold effectively.

8. **Annual Audits on Policies and Actual Practices.** This allows Compliance and Legal teams to assess whether existing processes and systems are adequate and to make adjustments as necessary.

In a recent survey\(^{10}\), 81% of the respondents said that they expected their company to have to deal with more incidents of misuse of social communications. This demonstrates a real need for action by organisations today to ensure that the risk posed by the use of electronic communications is identified and policies, processes, and technology put in place to mitigate those risks.

## Recent Examples of Misuse of Electronic Communications

<table>
<thead>
<tr>
<th>Case</th>
<th>What happened?</th>
<th>Electronic Communications Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forex scandal</td>
<td>Currency traders across several financial institutions formed a ‘cabal’ to fix foreign exchange rates.</td>
<td>Private chat rooms</td>
</tr>
<tr>
<td>LIBOR scandal</td>
<td>Traders colluded with benchmark setting colleagues to manipulate LIBOR</td>
<td>Instant Message</td>
</tr>
<tr>
<td>PayPal Incident</td>
<td>Disparaging comments about colleagues led to dismissal of a high profile PayPal executive.</td>
<td>Twitter</td>
</tr>
<tr>
<td>Roberts v. IBM</td>
<td>Age discrimination with HR referring to employee’s “shelf life”</td>
<td>Instant Message</td>
</tr>
<tr>
<td>Lord McAlpine v Sarah Bercow</td>
<td>Defamatory allegation shared on Twitter; First High Court Twitter libel trial in UK.</td>
<td>Twitter</td>
</tr>
<tr>
<td>Whitmar v Gamage &amp; Others</td>
<td>Unfair competition; corporate LinkedIn account hijacked by ex-employee to win customers over to a competitor.</td>
<td>LinkedIn</td>
</tr>
<tr>
<td>Gosden v Lifeline Project Ltd</td>
<td>Breach of equal opportunity policies; chain email containing racist and sexist content sent and receiver encouraged to ‘Send it on’.</td>
<td>Email</td>
</tr>
<tr>
<td>Ghali v Transperfect Transla-</td>
<td>Discrimination – national origin; derogative comments made on instant message by employees seen by a colleague.</td>
<td>Instant Message</td>
</tr>
<tr>
<td>tions limited (2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zynga v Alan Patmore (2012)</td>
<td>Employee copied and took confidential information to competitor when he resigned.</td>
<td>Public email, cloud share</td>
</tr>
</tbody>
</table>

## Appendix 1: Regulations Relevant to Electronic Communications

### Record Retention

<table>
<thead>
<tr>
<th>Regulator</th>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UK</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCA</td>
<td>COBS 11.5 Record keeping: client orders and transactions</td>
<td>Records of client details, orders placed, who dealt with the order, what was executed, and any transactional prices.</td>
</tr>
<tr>
<td>FCA</td>
<td>COBS 11.8 Recording telephone conversations and electronic communications</td>
<td>Firms to record relevant telephone conversations, and keep a copy of relevant electronic communications, sent between the firm and their client or client’s representative. These need to be preserved in an easily accessible location, for at least 6 months from the date the record was created, and in a tamper-proof format.</td>
</tr>
<tr>
<td>FCA</td>
<td>Policy Statement 08/1 – Telephone Recording: recording of voice conversations and electronic communications, FSA, March 2008</td>
<td>Clarifies the meaning of electronic communications giving it a broad definition including fax, email, Bloomberg mail, video conferencing, SMS, business to business devices, chat and instant messaging and extends to include new technologies that come online.</td>
</tr>
<tr>
<td>FCA</td>
<td>SYSC 9 Record-keeping</td>
<td>Records should be stored in a readily accessible place, in a tamper-proof format. SYSC 9 makes reference to the obligations that firms have under MiFID and the UCITS Directive (from the European Commission), such as keeping related business records for a period of at least five years.</td>
</tr>
<tr>
<td><strong>Switzerland</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FINMA</td>
<td>Market Conduct Rules</td>
<td>Retention of all electronic communications sent by employees in securities trading and be able to produce electronic communications sent by employees in securities trading to FINMA without alteration.</td>
</tr>
<tr>
<td><strong>EU</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESMA</td>
<td>MiFID II Article 16(7)– Recording of Telephone Conversations and Electronic Communications</td>
<td>Telephone conversations or electronic communications relating to investment services have to be recorded. ESMA clarifies that this could include internal calls where the call “relates to or is intended to result in transactions”.</td>
</tr>
<tr>
<td>CFTC</td>
<td>Dodd-Frank Act – Section 731</td>
<td>Daily trading records of swaps and all related records (including related cash or forward transactions) and electronic communications, including electronic mail, instant messages, and recordings of telephone calls, have to be retained for a period as may be required by the Commodity Futures Trading Commission (CFTC), currently one year. This information needs to be stored safely and in a manner that allows for easy retrieval and review by regulators.</td>
</tr>
</tbody>
</table>