Mutual Fund Dealers Association of Canada
Association canadienne des courtiers de fonds mutuels

Contact: Ken Woodard
Director, Communications & Membership Services
Phone: 416-943-4602
E-mail : kwoodard@mfda.ca

BULLETIN #0744-C
March 29, 2018

MFDA Bulletin

Compliance

For Distribution to Relevant Parties within your Firm

Electronic Communications Review

The MFDA continues to work to raise awareness of current risks associated with the use of technology and to increase MFDA understanding of Member practices. With this in mind, in 2017 MFDA staff issued a survey asking Members to provide details on the use of electronic communications with clients.

The attached report summarizes our observations and provides recommendations to Members.

DM #602653

Electronic Communications Review

March 29, 2018

DM#596419

INTRODUCTION

Members have used email to communicate with clients for many years. Since this time, the technology of communicating electronically with clients has expanded rapidly and a number of these technologies provide more secure alternatives to "traditional" email communications.

There are four main areas of risk when it comes to electronic communications: books and records (including evidence of client authorization), supervision of Approved Person (AP) activity, general security, and protection of confidential client information.

The MFDA continues to work to raise awareness of current risks associated with the use of technology and to increase MFDA understanding of Member practices. With this in mind, in 2017 MFDA staff issued a survey asking Members to provide details on the use of electronic communications with clients. This included the use of personal email, delivery of confidential client information, and electronic receipt of client instructions/authorization.

This report outlines observations and provides recommendations to Members.

RELEVANT RULES

Rule 5: Books and Records

Members are required under MFDA Rule 5.1 (Requirements for Records) to "keep such books, records and other documents as are necessary for the proper recording of its business transactions and financial affairs and the transactions that it executes on behalf of others and shall keep such other books, records and documents as may be otherwise required by the Corporation."

In addition, MFDA Rule 5.2 (Storage Medium), MFDA Rule 5.5 (Access to Books and Records) and MFDA Rule 5.6 (Record Retention) set out the requirements for maintaining, and providing to the MFDA, such books and records.

Rule 2.1.3: Confidentiality and Protection of Client Information

All information Members receive relating to clients must be kept confidential in accordance with MFDA Rule 2.1.3 (Confidential Information). MFDA Rule 2.1.3 (b) requires Members to develop and maintain policies and procedures relating to confidentiality and the protection of information held by it in respect of clients.

MFDA Rule 1.4 and Policy 6: Reporting Requirements

MFDA Rule 1.4 requires Members and Approved Persons to report information to the MFDA within specified time periods. MFDA Policy 6 provides further clarification of the specific information Members and Approved Persons must report to the MFDA using the MFDA's Member Event Tracking System (or "METS"). MFDA Policy 6 Part B section 6.1(b)(ii) requires Members and Approved Persons to report a breach of client confidentiality on METS within 5 business days of the occurrence.

GENERAL COMMENTARY AND OBSERVATIONS

Email

Personal Email and/or Text

The majority of respondents advised that they have policies to restrict the use of personal email and/or text for Member business. Other Members advised that they do not have a policy in place but they have corporate email available to all Approved Persons and discourage the use of personal email.

Some Members advised that they have policies to monitor for the use of personal email and/or text including testing during branch examinations. One Member that allows email through AP trade name entity email accounts stated that, as a control, they apply keyword filtering and an archiving solution.

Email Delivery of Confidential Client Information

The majority of Members advised that they do allow email and/or text delivery of confidential client information, but only through corporate email. Members reported additional controls for delivery such as encryption and passwords. Encryption was exclusive to those that only allowed delivery through corporate email. For passwords,

Members outlined various policies and procedures such as their creation and strength requirements.

Some Members allow delivery of confidential client information through the Member's back office service provider's system. This system automatically generates emails notifying clients that reports are available to be accessed through a secure web portal.

Some Members advised they do not allow email and/or text delivery of confidential client information and have controls in place to monitor for such delivery, including the use of keyword monitoring and Data Loss Prevention (DLP) software.

Concerns with the use of email

There are a number of concerns with the use of email for communicating with clients.

Use of Non-Member email

As noted above, the Member is required to keep, and furnish to the MFDA upon request, such books, records and other documents as are necessary for the proper recording of its business transactions and financial affairs and the transactions that it executes on behalf of others and shall keep such other books, records and documents as may be otherwise required by the Corporation. Communications with clients regarding Member business constitute Member books and records and must be maintained. Such maintenance is made significantly more difficult if APs are not using the Member's corporate email accounts.

Email must be appropriately secured in order to protect from events such as hacking and privacy breaches. If the Member does not have control of the email system being used, they do not have control of the security settings such as passwords and encryption nor can they monitor for cybersecurity incidents such as phishing attacks. This could lead to breaches of not just the AP's computer, phone or other endpoint device, but the Member's own systems.

Additionally, Members are required to undertake appropriate supervision of APs, including their trading activity, marketing and outside business activities. Without access to complete books and records of the AP, such supervision may be incomplete and can impair the ability of supervisory staff to detect concerns or investigate issues that come to light via such avenues as client complaints.

Email Delivery

Members should be aware that any email system, especially when used to deliver confidential client information, can be of concern. Mis-delivery of information is a potential issue when the wrong client email address is selected or the email address is mis-typed. In addition, inadequate encryption and password protection can lead to breaches of client confidentiality.

Good Practices and Recommendations

- **Policies and procedures regarding the use of emails:**
  - **Requiring APs to use Member email when conducting Member business or otherwise have a system in place to capture all email correspondence regarding Member business**
  - **Ensure all email communications are encrypted and otherwise appropriately protected, including those sent via non-Member email**
  - **Rather than delivering confidential client information and documentation via email, consider using a secure Member web portal or cloud to deliver such information**

Web Portals

The majority of Members advised that they use web portals to deliver confidential client information. The delivery of confidential client information by web portal is preferable to email delivery as it is more secure, provided that adequate security (such as encryption and password protocols) is in place. Members advised that they had security protocols in place.

Members that use web portals will typically send email notifications advising clients that a document had been posted. Members also track some aspect of activity on the portal (any or all of: delivery, client access of the site, client viewing of documents and client download of documents).

Good Practices and Recommendations

- **Policies and procedures regarding use of web portals**
  - **Consider using a qualified third party (such as the Member's system provider) to host the web portal if the Member does not have adequate resources to host it themselves**

- **Have proper protocols for user ID and passwords including**
  - **Adequate set-up procedures, such as the process should be automated and/or occur at head office and prevent salespersons or assistants from creating passwords for clients**
  - **Minimum requirements for the password strength (length, use of numbers and special characters, etc.)**
  - **Consider frequency of changing passwords**
- **Tracking of access by clients**

- **Ensure there are adequate security protocols in place for the web portal in order to defend against cyber attacks**
- **When sending email notifications to clients that an item is posted to the web portal, ensure that it is encrypted and confidential client information is not included in the email. For example, the document posted should only appear on the web portal and not in the notification email.**

Reliance on Electronic Means for Client Authorization

A number of Members rely on electronic means to accept trade instructions, open client accounts or change client information. This could be through email instructions in the body of an email, documents with an original signature that are scanned and attached to an email, a client's physical electronic signatures captured on a tablet or other device or authorization through a web portal.

The most common method used was a document with an original signature that is scanned and attached to an email. Some Members advised that, for such signed instructions, they had specific restrictions on accepting them, including only accepting under a Limited Trading Authorization ("LTA") and/or an email agreement, or requiring verbal follow-up on at least redemption trades.

MFDA staff are of the view that, based on the risk involved in the use of email to accept client instructions, and the availability of technologies that allow for better means of client identification and security (such as e-signature technology or a password protected web-portal), Members should not accept client instructions via email. Client instructions typed in the body of an email do not constitute adequate evidence of client instructions, even where the client has signed an LTA.

Good Practices and Recommendations

- **In order to reduce risk to clients, APs and Members, email should not be used to solicit or accept client instructions. Instead, technologies that allow for better means of client identification and security should be used, such as a password protected web-portal.**

CONCLUSION

Members are reminded that any breaches of client confidentiality are required to be reported by the Member to the MFDA. This includes, but is not limited to, Member system breaches, mis-delivery of confidential client information, or compromised client email accounts that have resulted in the Member providing confidential client information to an unauthorized individual. Similarly, Approved Persons must report any such breaches to the Member.

We encourage Members to review the good practices and recommendations contained in this report, update their policies and procedures and provide staff training as required.

We will continue to assess Members' policies and procedures regarding electronic communications in future compliance examinations as it relates to maintaining books and records, evidence of client instructions and authorization, and confidentiality. Members with additional questions or those seeking guidance in enhancing their policies and procedures should contact their assigned MFDA Compliance Manager for further assistance.