Frozen Edition

This month, some people might be wondering if Queen Elsa snapped again and froze a good portion of North America. Figuratively, the government to the south of us froze shut for over a month as a political storm raged on. And now an actual wind is howling outside, as we face a new year with some new rules and fresh guidance. For private CBCA corporations, the past will be in the past soon (in June), when they'll have to start keeping share registers with detailed information about the significant, beneficial owners of their shares. And Ontario market participants are hopeful that the OSC's Burden Reduction Task Force will persuade the powers that be to let those unnecessary regulatory burdens go.

In this bulletin:

1. OSC Consults on Reducing Regulatory Burdens
2. SEC Settles Its First Enforcement Actions against Robo-Advisors
3. IIROC, the SEC, and FINRA Announce Their Compliance Priorities for 2019
4. New Share Register Requirements for Beneficial Owners with "Significant Control" Come into Force for Private CBCA Corporations this June
5. FINTRAC Updates Its Guidance on Suspicious Transaction Reports
6. FINRA Publishes Report on Effective Cyber-Security Practices

In Brief: OSC Invites Ontario Businesses to Participate in Global Launchpad

1. OSC Consults on Reducing Regulatory Burdens

On January 14, the Ontario Securities Commission (OSC) published Staff Notice 11-784 *Burden Reduction* (the Notice) to solicit feedback on steps that it can take to reduce regulatory burdens and improve the investor experience. This public consultation builds on the OSC's creation of a Burden Reduction Task Force (Task Force) with the Ontario Ministry of Finance last November.

The Task Force wants feedback on new initiatives that it should pursue, including the following:

- Are there operational changes that could be made to the regulatory branches, such as the Compliance and Registrant Regulation (CRR) Branch, to make market participants' interactions with the OSC easier or less costly, enhance certainty about regulatory requirements or outcomes, or reduce the unnecessary burdens associated with forms and filings?

In Brief

OSC Invites Ontario Businesses to Participate in Global Launchpad

On January 31, the Ontario Securities Commission (OSC) published a news release inviting innovative, Ontario businesses to apply for a pilot project (Pilot Project) to test financial products, services and business models across borders. Successful applicants will be able to simultaneously trial and scale their products or services in multiple jurisdictions and gain real-time insights into how they might operate in these markets. The application deadline is February 28, and the pilots are expected to run in the second half of 2019.

The Pilot Project is an initiative of the Global Financial Innovation Network (GFIN), which we wrote about in our August 2018 bulletin. Participating regulators in the Pilot Project include the British Columbia Securities Commission (BCSC), OSC and Autorité des Marchés Financiers (AMF) in Canada. Of potential interest to the asset management industry, regulators from financial centres in Bermuda, Dubai, Hong Kong, Guernsey, Jersey, Singapore and the United Kingdom are also participating, but the only participating U.S. regulator is the Consumer Financial Protection Bureau. If you want to find out more about the Pilot Project or submit an application, we can help. Please contact us.

- Are there any OSC rules that are inconsistent with rules in other jurisdictions and that could be harmonized?
- Are there OSC rules that no longer serve a valid purpose?
- What can the OSC do to enhance how investors experience disclosure before they invest?
- Are there any interim changes that the OSC could make to help market participants while it pursues national changes on a coordinated basis with other regulators?

This consultation supplements initiatives that the OSC and other members of the Canadian Securities Administrators (CSA) are pursuing to reduce regulatory burdens for reporting issuers. The Notice also indicates that the Task Force will consider relevant submissions made in respect of other initiatives, such as the proposed client-focused reforms, proposed amendments relating to embedded commissions for investment funds, and proposed regime for over-the-counter (OTC) derivatives. Accordingly, there is no need to repeat comments provided in response to these other projects.

Submissions are due by March 1, 2019. The OSC also plans to hold an initial roundtable on March 27, 2019 to consider the comments it has received. A comment letter is the price of admission to the roundtable.

After considering the suggestions it has received along with input from its advisory committees, the OSC intends to identify a series of short, medium and long-term actions to reduce regulatory burdens. There is no timeline indicated for this next step, but we expect that the Task Force will offer a progress report by the end of 2019.

AUM Law will monitor developments with respect to this initiative and keep you informed. If you are interested in making a submission, please contact us.

2. SEC Settles Its First Enforcement Actions against Robo-Advisors

In late December, the U.S. Securities and Exchange Commission (SEC) reached settlements with two robo-advisers, Wealthfront Advisors LLC (Wealthfront) and Hedgeable Inc. (Hedgeable). These cases, which are the SEC's first enforcement cases against robo-advisors, are of particular interest because they highlight some of the pitfalls for firms that use digital media as part of their marketing and communication strategies.

A. Wealthfront's Twitter Downfall

The Wealthfront settlement agreement shows how Wealthfront used problematic social media strategies without, in the SEC's view, adopting reasonably designed written policies and procedures for its marketing and investor communication activities. For example:

- Wealthfront used Twitter to post advertisements and communicate online with clients but didn't always preserve copies of the ads or retain communications made through its Twitter account relating to recommendations or advice given to clients.

- It re-tweeted positive posts by other Twitter users whom it knew or should have known had an economic interest in promoting Wealthfront, without disclosing these conflicts of interest. For example, some of the re-tweeted posts originally were made by Wealthfront employees, Wealthfront investors, and Wealthfront clients who received free services if a reader used the client's personalized landing page to enroll with Wealthfront. Its compliance policies and procedures did not ensure that all re-tweets were assessed by the Compliance Department for compliance with SEC rules before they were posted.
- For about a year, Wealthfront paid certain bloggers who successfully solicited new clients to open accounts, without the disclosures and documentation required under rules governing cash solicitations. Wealthfront also failed to comply with its own policies and procedures, which called for the chief compliance officer (CCO) to review and approve agreements with people soliciting clients under this program.

The SEC also asserted that Wealthfront made false statements about a tax-loss harvesting strategy that it offered to clients. It told clients that it would monitor all accounts for transactions that might trigger a wash sale, which can diminish the benefits of the harvesting strategy, but failed to do so.

Pursuant to the Settlement, Wealthfront agreed to pay a penalty of $250,000, entered into a cease and desist order regarding the problematic conduct, and undertook to provide each of its advisory clients with a copy of the settlement order.

B. Hedgeable

According to the Hedgeable settlement agreement, Hedgeable made misleading statements about its investment performance on its website and through social media. It purported to compare the investment performance of its clients with those of two robo-advisor competitors. However, the performance comparisons were misleading because Hedgeable included less than 4% of its client accounts, which had higher than average returns, and compared these returns with rates of return that weren't based on its competitors' actual trading models.

The SEC faulted Hedgeable for having an ineffective compliance program. Although Hedgeable's policies required employees to obtain the CCO's approval before sending any written communications to investors or prospective investors, this language wasn't broad enough to require the review of marketing and promotional material posted on digital media. During the relevant period, Hedgeable's CCO didn't know that social media posts were considered marketing materials under the Investment Advisers Act of 1940 (Advisers Act) and, consequently, did not review those posts.

Pursuant to the settlement agreement, Hedgeable agreed to pay a civil penalty of $80,000, was censured, and agreed to a cease and desist order. The relatively low penalty (and absence of a commitment to notify its clients of the settlement) may be because it was winding down its advisory business and reportedly had no assets under management as of September 2018.

C. Our Takeaway

These cases highlight the importance for firms that are (or considering becoming) active on social media to fully analyze how regulatory provisions may apply to social media and other digital media activities identify the potential risks, and draft policies and procedures that extend to these activities if they are subject to regulation. Of course, it's also important to train relevant employees so that they understand their compliance obligations and monitor these activities to detect and prevent non-compliance. AUM Law can assist you with all of these matters. Please contact us to learn how we can help.

3. IIROC, the SEC, and FINRA Announce Their Compliance Priorities for 2019

Recently, each of the Investment Industry Regulatory Organization of Canada (IIROC), the Office of Compliance Inspections and Examinations (OCIE) at the U.S. Securities and Exchange Commission (SEC) and the U.S. Financial Industry Regulatory Association (FINRA) published their compliance and exam priorities for 2019. Although these reports are of most relevance to the firms directly supervised by these regulators, we think that these supervisory trends will be of interest to Canadian firms as well.

We've created the table below to compare exam priorities that these organizations have identified and that we think are of potential interest to the asset management sector in Canada. We also included information about the compliance exam priorities that the Compliance and Registrant Regulation Branch (CRR) of the Ontario Securities Commission (OSC) identified in its annual report (OSC Report), which we wrote about in our August 2018 bulletin.

Please note that these organizations take different approaches to describing their compliance exam priorities. For example, FINRA's report describes its new exam initiatives for 2019 in detail. By contrast, the OSC Report lists only five, broad "focus areas" for its 2018-19 exams, but a deeper dive into that report indicates other areas of interest. For that reason, we've used two kinds of notation in the OSC column. Compliance priorities identified as a focus area for 2018-19 are marked with a "**19**". An "**18**" marks the broad focus areas from the 2017-18 exam cycle as well as specific deficiency areas from 2017-18 that are similar to exam priorities that IIROC, the SEC and/or FINRA have flagged for the coming year. Links to the organizations' reports are included in the table heading below.

Theme	OSC	IIROC	SEC	FINRA
Anti-money laundering (AML) compliance				
General			X	
Customer due diligence, including verification of beneficial owners				X
Business conduct (including conflicts of interest)				
Affiliated service providers and products	18		X	
Best execution	18	X		X
Borrowing from clients			X	
Compensation-related conflicts	19	X	X	
Fees and expenses (*e.g.* which expenses can be charged to funds, appropriate disclosure of fees and costs of investing)	18		X	
Market access, short sales and short tenders				X
Market manipulation – manipulative trading in correlated exchange-traded products (ETPs) and/or correlated options products				X
Outside business activities – general		X		X
Outside business activities – raising funds from customers away from firm's supervision				X
Referral arrangements	18			
Retail fund sales practices	19			

Theme	OSC	IIROC	SEC	FINRA
Securities-backed non-purpose loans and lines of credit			X	
Business models				
Advisers that provide advice to private and public funds with similar strategies			X	
Dealers that sell microcap stocks			X	
Online or automated business models		X		X
Order-execution-only (OEO) platforms		X		
Retail funds with riskier profiles (*e.g.* funds with higher allocations to securitized assets, funds with aberrational underperformance)			X	
Client reporting and disclosure				
General	18			
Deficiencies in client reports	18			
Fixed income mark-up disclosure				X
Offering memorandum exemption – dealer delivery	18			
Cyber, Digital and Tech Developments				
Cybersecurity - general		X	X	X
Cybersecurity – advisers with multiple branches		X	X	
Cybersecurity – configuration of network storage				
Cybersecurity – retail trading information security			X	
Digital asset businesses – controls and supervision			X	X
Regtech for compliance				X
Referral arrangements	18			
Retail fund sales practices	19			
Securities-backed non-purpose loans and lines of credit			X	
Financial condition and operational matters				
Financial condition – general	18			X
Credit risk management				X
Customer account guarantees		X		
Liquidity planning, including updates to stress tests in light of marketplace changes and increased volatility				X
Outsourcing arrangements	18			
Retail funds – oversight by their boards	18		X	
Safeguarding clients' assets	18		X	
Service arrangements between dealers and portfolio managers		X		

Theme	OSC	IIROC	SEC	FINRA
Trading – electronic trading controls, supervision with trading rules		X		
Higher-risk firms and products				
Education – non-compliance with post-registration education requirements, etc.		X		
Firms that haven't been audited recently			X	
Firms employing individuals with problematic history			X	
New registrants	19		X	
Retail funds with risky profiles (*e.g.* ETFs with little secondary market trading volume and smaller assets under management, funds with higher allocations to securitized assets, funds with aberrational underperformance relative to peers, and funds that track bespoke indices)			X	
Self-assessments or prior audits that reveal higher compliance risks (including firms with repeated filing deficiencies)	19	X		
Senior and vulnerable clients				
Senior investors – general	18		X	
Senior investors – identifying and handling financial exploitation			X	X
Senior investors – obtaining trusted contact information				X
Know-your-client (KYC), Know-your-product (KYP), and Suitability				
General	18		X	X
Quantitative suitability determinations and supervisory controls				X
Novel or complex exchange-traded products			X	X
Over-concentration in illiquid securities				X
Portfolio management and trading practices (*e.g.* suitability, alignment with disclosures, adequacy of risk disclosure, monitoring of attendant risks)			X	
Products that package leveraged loans				X
Recommendations to buy share classes not in line with customer's investment horizons				X
Other				
Appropriate accounting standards	18			
Whistleblower regime – employment agreements that are offside the prohibition on reprisals	18			

4. New Share Register Requirements for Beneficial Owners with "Significant Control" Come into Force for Private CBCA Corporations this June

Beginning June 13, "non-distributing corporations" organized under the Canada Business Corporations Act (CBCA) will have to collect and maintain in a share register detailed information about individuals with "significant control" over the corporation. These changes to the CBCA (Amendments) reflect the federal government's commitment to enhance transparency over beneficial ownership of companies and might serve as a model for similar changes to corporate legislation in Canadian provinces and territories.

Background: In 2016, the Financial Action Task Force (FATF) criticized Canada's corporate law regime for regulatory gaps relating to the quality and reliability of beneficial ownership information for legal entities and partnerships. For example, although CBCA corporations have to maintain share registers, these registers only need to include the names and addresses of registered security holders, not beneficial owners. According to FATF, gaps like these increase the risk of money laundering and terrorist financing by permitting nominee shareholders and trusts to conceal the identity of beneficial owners.

In December 2017, Canada's federal, provincial and territorial ministers of finance agreed in principle to pursue legislative amendments to ensure that corporations hold accurate and up-to-date information on beneficial owners that will be available to authorities. And, as we discussed in our November 2018 bulletin, the House of Commons Standing Committee on Finance released a report recommending that the authorities create a pan-Canadian beneficial ownership registry, accessible to law enforcement agencies, that covers all legal persons or entities having at least a 25% of total share ownership or voting rights in Canadian companies or foreign companies that own property in Canada. The Amendments represent a step toward this goal, at least at the federal level.

Which Corporations Are Subject to the Amendments? The Amendments apply to federal, non-distributing corporations, *i.e.* private corporations. A non-distributing corporation is a corporation established under the CBCA that:

- is not a reporting issuer in any jurisdiction in Canada;
- has not filed a prospectus or registration statement in Canada or elsewhere;
- does not have any securities listed or posted for trading on a stock exchange inside or outside Canada, and
- is not a successor to a distributing corporation.

Reporting issuers in Canada, and significant beneficial owners of reporting issuers' shares in Canada, are already subject to securities legislation (such as the early warning regime and insider reporting obligations) that provide more transparency in this area, and so this is why "distributing corporations" are exempt from the Amendments.

Which Shareholders Will Be Identified in the Share Register? Corporations will have to identify and maintain detailed information in a securities register about individuals with "significant control" over the corporation. Significant control is defined to mean an individual:

- Who is the registered or beneficial owner of, or has direct or indirect control or direction over, any number of shares that either carry 25% or more of the voting rights attaching to all of the corporation's outstanding voting shares or represent 25% or more of all of the corporation's outstanding shares measured by fair market value (Significant Number of Shares);

- Who has any direct or indirect influence that, if exercised, would result in control in fact of the corporation; or
- To whom prescribed circumstances (which haven't been specified yet) apply.

Individuals with direct or indirect joint ownership, control or influence over a Significant Number of Shares will each be considered an individual with significant control under the Amendments.

Which Information Must Be Collected and Maintained? The corporation will have to maintain a share register in Canada containing detailed information about individuals with significant control over it, including:

- The individual's name, birthdate and latest known address;
- Their jurisdiction of residence for tax purposes;
- A description of how the individual qualifies as having significant control;
- The date on which each individual became or ceased to be an individual with significant control; and
- Steps taken to identify all individuals with significant control and ensure that the information is kept up-to-date.

Who Gets Access to the Information? The corporation will have make this information available to its shareholders and creditors, upon request, to use for matters relating to the corporation's affairs. Furthermore, although corporations subject to these new requirements will not have a pro-active duty to report this information to authorities, the Director appointed under the CBCA can request it.

Keeping the Information Up-to-Date: The corporation has several requirements to keep the information up-to-date:

- At least once every financial year, the corporation will have to take reasonable steps to ensure that it has identified all individuals with significant control over the corporation and that the information in the register is accurate, complete and up-to-date.
- It must update the share register within fifteen days of becoming aware of any information it is required to collect and maintain.
- Within one year after the sixth anniversary of the day an individual ceases to be a significant shareholder, the corporation must dispose of that individual's personal information (unless other legislation in Canada requires the information to be kept for a longer period of time).

Shareholders Have Obligations, Too? If a corporation requests any of the information it is required to collect and maintain in the share register from one of its shareholders, the shareholder is required to reply accurately and completely, to the best of their knowledge, as soon as feasible.

What Happens Next? Corporations Canada is expected to enact regulations that indicate how to create and maintain the register before the new requirements come into force on June 13, 2019.

Since all of the Ministers of Finance agreed in principle to pursue similar legislative amendments, we think it is likely that similar changes will be made to corporate statutes in provinces and territories over time. The commitment, however, was of the "we'll try" rather than "we'll do it" variety, so there is no clear timeline for change.

If your firm is subject to the Amendments and you would like assistance implementing these new requirements, please contact us. AUM Law also will be monitoring legislative trends in this area and will report on future developments.

5. FINTRAC Updates Its Guidance on Suspicious Transaction Reports

On January 17, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) updated its guidance on suspicious transaction report (STR) requirements under Canada's anti-money laundering and anti-terrorist financing (AMLTF) regime. The new guidance covers the following subjects:

A. What Is a Suspicious Transaction Report?

This publication outlines how to identify a suspicious transaction, what an STR is, and the important role that STRs serve in Canada's AMLTF regime. It includes a useful framework for identifying suspicious transactions and determining whether they trigger the STR threshold. An STR must be filed if there are "reasonable grounds to suspect" that a transaction is related to the commission or attempted commission of a money laundering (ML) or terrorist financing (TF) offence. FINTRAC distinguishes among the following thresholds:

- A "simple suspicion" is a hunch or intuition that ML or TF is occurring. It doesn't trigger a reporting obligation but could prompt a firm to assess similar transactions to see if there are other facts, context or ML/TF indicators (discussed in more detail below) to confirm the suspicion.
- If a firm, based on its assessment of facts, context and ML/TF indicators, concludes that it is **possible** that a transaction is related to the commission of ML or TF, then it has "reasonable grounds to suspect" ML or TF, and an STR must be filed.
- "Reasonable grounds to believe" exist when ML or TF **probably** is occurring, and the firm can present a set of verified facts that can be proven to support this suspicion. A firm need not, and **should not**, wait until it has a "reasonable grounds to believe" that ML or TF is occurring before it files an STR.

This publication also provides guidance on how FINTRAC assesses, and how firms can assess, their compliance with the STR requirements. FINTRAC suggests that firms consider the following elements, among others:

- Can the firm explain how its process for detecting, assessing and reporting suspicious transactions is reasonable, effective and consistent in light of the firm's risk assessment?
- Although firms aren't required to document their rationale for why they didn't file an STR for an unusual transaction, such records "may be useful in the context of a FINTRAC assessment." (In other words, expect an uncomfortable FINTRAC audit if you don't create and retain this documentation.)
- Is the firm continuing to submit STRs for clients in respect of whom the firm has already submitted an STR (unless and until the firm determines that there are no longer reasonable grounds to suspect ML or TF)?
- Is the firm reviewing files to determine, among other things, that filing deadlines are being complied with, that STRs are sufficiently detailed, and that similar transactions are being treated consistently for assessment and STR purposes?

B. Reporting Suspicious Transactions to FINTRAC

This publication provides detailed guidance on how to complete STRs. It describes when a suspicious transaction must be reported, what FINTRAC expects to find in STRs, and how to submit reports using

FINTRAC's secure website F2R. Reports must be filed electronically if you have the capability; otherwise, they can be submitted on paper. Service providers can submit reports on a reporting entity's behalf, but the reporting entity remains legally responsible for compliance.

This guidance also describes common STR deficiencies to avoid, such as using a higher threshold for reporting (such as "reasonable grounds to believe" that the transaction is related to commission or attempted commission of an ML or TF offence, instead of "reasonable grounds to suspect"), failing to list all of the relevant transactions and accounts, failing to list all parties to the transaction where the information is available, and/or failing to articulate the reasons for determining that there are reasonable grounds to suspect ML or TF.

C. ML and TF Indicators

FINTRAC has published industry-specific guides to ML and TF indicators, including guidance for "security dealers." FINTRAC expects to see firms use these ML and TF indicators in their STR program but also stresses that these indicators are not an exhaustive list to support all suspicious scenarios.

FINTRAC emphasizes the importance of considering facts, context and ML/TF indicators when assessing a suspicious transaction. It is significant that the new guidance states:

> "On its own, a single transaction or ML/TF indicator may not appear suspicious. However, this does not mean you should stop your assessment. Additional facts or context about the associated individual or their actions may help you reach the reasonable grounds to suspect threshold."

This quote should be read together with the guidance in *What is a suspicious transaction report?*, which recommends that firms document their reasons for negating suspicions about a transaction. Read together, these guidance documents suggest that firms keep appropriate records of their reasons for not filing an STR in respect of transactions or situations where there is only a single ML/TF indicator present.

Next Steps: If you have questions about the updated guidance or any other ML/TF compliance matters, please contact us. AUM Law can help you review and update your policies and procedures to reflect the new guidance as needed, provide training to your employees, and provide legal advice on applying the STR requirements and guidance to specific fact situations.

6. FINRA Publishes Report on Effective Cyber-Security Practices

On December 20, the U.S. Financial Industry Regulatory Authority (FINRA) published its Report on Selected Cybersecurity Practices (Report), describing effective practices that it has observed among the broker-dealer firms that it supervises. Cybersecurity continues to be a high priority, regulatory compliance issue north of the border, and so we think that the Report is a worth a read for Canadian registrants, too. Based on the report, we've outlined some questions below for firms to consider:

Mobile devices: The proliferation of mobile devices increases the risk of data loss. Does your firm have appropriate policies and procedures to regulate risk for mobile devices used by employees, such as bring-your-own-device standards, security settings, encryption, passwords, physical security, reporting procedures for lost devices, and capacity to remotely wipe firm data for devices that have been lost or belong to former employees? Depending on their business model, firms also should consider whether there are steps they should take regarding their customers, such as:

- monitoring mobile application markets on the dark web for malicious applications that impersonate the firm's mobile application;

- informing customers about the risks of accessing and storing personal and financial data on their mobile devices; and/or
- restricting certain changes to account settings via mobile device and requiring customers to contact the firm to make such changes.

Insider threats: Either intentionally due to malicious behavior or inadvertently (*e.g.*, a laptop lost in a Lyft), insiders pose a serious threat to cybersecurity. Does your firm have the right amount of technical controls (including effective identity access management and user entitlement processes), additional controls for privileged users, data loss prevention (DLP) controls (*i.e.*, that identify sensitive customer or firm data and then block or quarantine its transmission), training, measures to identify potentially abnormal user behaviour in the network, and adequate supervision?

Penetration testing: Testing cybersecurity policies and procedures is an important part of any compliance program. Would penetration testing (*i.e.*, a simulated attack on the firm's computer network) to validate your policies and procedures be appropriate for your firm? One factor to consider in assessing the relevance of penetration testing (and which type of test, if any, should be conducted) is the degree to which the firm manages or stores confidential or critical data such as trading strategies, customers' personal information, and/or confidential information about other entities (such as information about mergers and acquisitions).

Branch Controls: Does your firm have more than one office? If so, it may be appropriate for you to assess:

- Whether you have adequate cybersecurity policies, procedures and technical controls that address the risks arising from branch office structures;
- The quality of your asset inventories (*e.g.*, that identify where sensitive customer and firm information is stored) and whether you're ensuring security of physical assets and providing for secured asset disposal at your branches;
- Whether your reviews of branch office operations encompass compliance with cybersecurity policies and procedures.

Even if you don't have branch offices, some of the considerations listed in the Report relating to branch offices (*e.g.*, ensuring minimum encryption standards as well as regular patching, anti-virus and malware protection and operating system updates for hardware used to access firm systems) may be relevant if you have employees that work remotely.

Phishing: Social engineering or "phishing" attacks continue to be one of the most common cybersecurity threats faced by firms. Measures a firm may wish to consider taking to address these risks include the following:

- Do you have appropriate technology in place to prevent as many attacks as possible and reduce the impact of successful attacks? In our view, it's not a question of if your firm will be hit. It's a question of **how prepared you are.**
- Do you including phishing scenarios in the firm-level, risk assessment process?
- Do you conduct regular, simulated phishing campaigns to evaluate employee understanding of and compliance with firm policies and procedures?
- Do you conduct remedial training and impose appropriate consequences for employees who repeatedly violate the firm's policies or do not demonstrate sufficient sensitivity to phishing risks during the firm's simulated phishing campaigns?

The Report includes a pair of useful charts to remind readers of: (1) the kinds of trustworthy entities or individuals that attackers often seek to disguise themselves as; and (2) the hallmarks of phishing communication. When you read these reminders, it's hard not to say, "Duh, that's obvious." But it's surprisingly easy to forget the obvious when a well-crafted phishing email pops up on your screen. So, for your convenience, we've reproduced the charts for you below, so that you can pin them to your bulletin board.

Phishes Often Appear to Come from A Trustworthy Source	
Entities	**Individuals**
Firm or affiliate	Friends
Government agencies, such as the U.S. Securities and Exchange Commission, FINRA and the IRS	Customers
Banks and other financial institutions	Information Technology (IT) administrators and Help Desk representatives
Social media sites	Office managers
Auction sites	Senior executives
Online payment processors	CEO or CFO

Hallmarks of Phishing Communications	
Category	**Characteristics**
Sender	Discrepancies between the name and email address or "reply to" address of the sender
	Unknown individual or corporation
	New individual with whom you do not regularly correspond, such as IT manager, senior manager or CEO of the organization
Recipients	Additional unknown recipients
Content	Generic salutations
	Unexpected timing, type or style of communication from a known sender, such as a friend, co-worker or boss
	Problems with grammar or spelling, including subtle character substitutions, such as 0 (zero) in place of O (the letter O), or 1 (the digit one) in place of l (lower-case L)
	Request for highly sensitive information, such as customer account lists, Social Security numbers, credit card numbers, user names or passwords
	Sense of urgency with a request to access links or attachments, provide personal information or initiate a transaction (FINRA observes this frequently in the context of fraudulent wire transfer requests)
	Pressure to bypass or ignore firm policies or procedures
	Notifications that are "too good to be true" (such as winning the lottery or receiving an inheritance)
	Content that is designed to induce an emotional reaction in the recipient, such as political messages, personal attacks or untrue accusations

Attachments and Links	Unexpected attachments, apps or links
	Discrepancy between the written address of the link and its true destination (determined by hovering over the link)
	Suspicious URL patterns where the name of the intended website appears anywhere other than at the very beginning of the URL
	Upon visiting the site, a message indicates a problem with the "certificate"

FINRA, *Report on Selected Cybersecurity Practices* (2019)

AUM Law can help you assess and enhance your cybersecurity policies and procedures and conduct compliance training in this area for your employees. Please contact us to find out more about our services in this area.

Practical Advice. Efficient Service. Fixed-Fee Plans.

AUM Law focuses on serving the asset management sector in the areas of regulatory compliance and investment funds. We also support clients in this sector by providing legal advice and services for structuring entities, raising capital, business combinations, and compliance with reporting issuers' and investors' disclosure obligations. Our clients include investment fund managers, portfolio managers, dealers, public and private investment vehicles including real estate funds, alternative funds and private equity funds, investors, and private and public companies.

This bulletin is an overview only and it does not constitute legal advice. It is not intended to be a complete statement of the law or an opinion on any matter. No one should act upon the information in this bulletin without a thorough examination of the law as applied to the facts of a specific situation.