Digital Engagement Practices:

Dark Patterns in Retail Investing

Contents

Executive Summary

In an increasingly competitive landscape, investing platforms for self-directed retail investors are adopting new digital marketing, engagement, and design techniques to influence investors' behaviour. Many of these techniques have generated regulatory concerns due to their potential impact on investors' financial wellbeing and privacy protections.

Building on findings from the Ontario Securities Commission's (OSC) previous report, "Digital Engagement Practices in Retail Investing: Gamification and Other Behavioural Techniques," this report examines a subset of digital engagement practices that includes **dark patterns, dark nudges, sludge, and targeted advertising**.

What are these techniques?

- **Dark patterns** are defined as user interface choices that manipulate, steer, or deceive users into making decisions that benefit the firm but may not align with users' best interests or personal preferences.

- **Dark nudges** are defined as nudges that make it easy for consumers to make choices that decrease their welfare.

- **Sludge** is defined as elements within a user interface that actively impede activities that are in the consumers' best interest, resulting in a reduction of welfare.

- **Targeted advertising** is a form of online advertising. It is defined as a digital marketing practice that uses data about individuals to select and display ads or other forms of commercial content.

What is in the report?

Recognizing the potential risks these techniques create for investor protection, the OSC Investor Office and the Behavioural Insights Team partnered to help examine their impact on retail investing. The OSC and BIT have reviewed and summarized the current state of research on dark patterns, dark nudges, sludge, and targeted advertising, the extent to which those techniques are in use on trading platforms, and how regulators in Canada, the US, and the EU are responding.

We have produced a set of definitions through this systematic research as well as a detailed, wide-ranging classification of specific techniques that fit under the categories of dark patterns, dark nudges, sludge, and targeted advertising. Within our research, we identified seven types of dark patterns, two types of dark nudges, and two forms of sludge:

Dark Patterns	
Technique	Definition
1. Prompts and reminders	Prompts are brief visual, graphic, or auditory stimuli that grab the user's attention to encourage specific behaviours or choices. Reminders are a specific type of prompt that follow up on a previous interaction or engagement.
2. Intermediate Currency	Intermediate currencies obscure the price of an item by providing it in a currency other than the normal, predominant currency.
3. Ranking	Ranking refers to setting the order that options are presented on a user interface in a way that privileges or promotes certain choices.
4. Sensory Manipulations	Sensory manipulations refer to changes to the user interface that focus the user's attention on one thing to distract them from something else.
5. Social norms and interactions	Social norms and interactions refer to two related sets of techniques that leverage how people look to the behaviour of others for cues on their own choices.
6. Scarcity claims	Scarcity claims are statements that a product or service will not be available for long due to limited supply, pending price increases, or other factors.
7. Hidden fees / information	Information about fees or other important platform features like privacy protections can be "hidden" through outright omission, delayed disclosure, or complex language, among other means.
Dark Nudges	
Technique	Definition
8. Removal of process steps	Practices that make it easier for users to make inadvertent or ill-considered decisions by removing the requirement for one or more actions (e.g., confirmations).
9. Defaults	A default is a preselected setting that automatically takes effect unless users actively change it.
Sludge	
Technique	Definition
10. Process frictions	People tend to procrastinate or avoid tasks when they are deemed challenging, tedious, or boring. Sludge plays to this tendency by creating 'psychological fences' that impede an individual's ability to get things done.
11. Complex language	The use of technical, overly complex (e.g., 'legalese'), or lengthy language to confuse or distract the user.

In our research, we found that the existing evidence base surrounding these techniques has enormous gaps, given the rapid pace of change in the industry and the relatively sparse data that platforms have shared with researchers and the public. We also found that dark patterns are particularly prevalent and have the potential to negatively impact investor welfare. Areas of particular concern include techniques that disguise the cost of investing (e.g., hidden fees and information), obtain personal information without informed consent, and make it harder to withdraw funds, close an account, or stop a premium subscription service.

More broadly, our research revealed potential risks created by dark patterns, dark nudges, sludge, and targeted advertising:

- Requiring users to **opt-in to certain features that can constitute dark patterns or dark nudges,** including most prompts (e.g., price movement notifications) and ranked lists (e.g., platform-specific top-traded lists).

- **Obtaining data without informed consent that is used for targeted advertising.**

- **Targeted advertising by investing platforms to vulnerable customers, including people with cognitive limitations and users likely to be new to or unfamiliar with online environments**.

- **Complex language** within fee schedules, privacy protections, and restrictions on withdrawing funds.

- **The removal of process steps in trade execution, making it less likely people will deliberate about a trade before they execute it.**

- The **difficulty for customers to cancel subscriptions, close accounts, and withdraw funds.**

Introduction

More platforms are available to self-directed retail investors than ever before. Across digital assets and traditional securities, there is fierce competition in the marketplace and a proliferation of new approaches to acquire and retain customers, and to maximize revenue from those customers.

Some of these approaches have raised the alarm of regulators, who have articulated concerns that potentially deceptive, misleading, or manipulative user engagement and experience design techniques are negatively impacting investors and contravening regulations. These techniques of concern include practices commonly labelled as dark patterns, dark nudges, sludge, and targeted advertising. Globally, regulators are considering the adequacy of existing investor protection legislation and regulation and the potential need for new regulatory and non-regulatory tools.

Regulators are limited by limited evidence regarding which of these practices are truly problematic for investor outcomes and how they can be mitigated. There are often differing understandings among regulators and stakeholders on the definition of key terms including "dark patterns." Most of the available evidence comes from other consumer domains, like the retail sector. While relevant, the complexity of financial products and the impact of investment decisions on long-term financial wellbeing means that the retail investing space is truly a special case.

In this challenging context, the Ontario Securities Commission (OSC) partnered with the Behavioural Insights Team (BIT) to answer a series of related questions including:

- How are dark patterns, dark nudges, sludge, and targeted advertising being employed by investing platforms?

- How are these digital engagement practices influencing retail investor attitudes and behaviour, and how can any negative impacts be mitigated?

- How are Canadian, US and other international regulators responding to these practices?

To answer these questions, we developed and implemented a mixed-methods research approach with the following key activities:

1. **Defined the key terms** (dark patterns, dark nudges, sludge, and targeted advertising) and mapped their relationship to each other based on existing definitions, refined to reflect a retail investing context.

2. **Conducted a literature scan** to develop an **initial taxonomy** of the specific practices that fit under each key term. This included a review of 37 sources, including peer-review publications and "gray" literature (i.e., non-peer-reviewed publications).

For each practice, we developed a definition and a summary of the impact of the technique on consumer / investor behaviour.

3. **Conducted a review of 10 investing platforms** (i.e., an environmental scan between November 2022 to January 2023) to identify which of the practices from the taxonomy are present on specific platforms and how / when they are being implemented. Platforms included major online trading and investment services, including regulated and unregulated crypto trading firms. The review also revealed additional techniques that were not identified in the literature review; these were subsequently included in our **final taxonomy of 11 specific techniques** across the broader categories of dark patterns, dark nudges, and sludge**.** Targeted advertising represents an additional, standalone category.

Classification: Dark Patterns, Dark Nudges, Sludge, and Targeted Advertising

Overview

A broad range of digital engagement practices (DEPs) are being employed by investing platforms. Drawing on the definition previously used in our Digital Engagement Practices report[1], DEPs are tools including behavioural techniques, differential marketing, gamification, design elements, or design features that intentionally or unintentionally engage with retail investors on digital platforms, as well as the analytical and technological tools and methods.[2] Dark patterns, dark nudges, and sludge are also types of DEPs. Classifying and categorizing these practices enables better organization of research findings and policy recommendations. As illustrated in Figure 1, below, this report examines two sets of DEPs: Online Choice Architecture (OCA), which relates to the design of the platform itself, and targeted advertising, which relates to certain marketing activities outside of the platform.

Figure 1: The relationship between digital engagement practices, online choice architecture, and targeted advertising.

---

[1] Ontario Securities Commission (2022). OSC Staff Notice 11-796 - Digital Engagement Practices in Retail Investing: Gamification and Other Behavioural Techniques.

[2] This definition was based on the U.S. Securities and Exchange Commission's definition of Digital Engagement Practices; U.S. Securities and Exchange Commission (2021). SEC Requests Information and Comment on Broker-Dealer and Investment Adviser Digital Engagement Practices, Related Tools and Methods, and Regulatory Considerations and Potential Approaches; Information and Comments on Investment Adviser Use of Technology.

We began developing this classification by defining the key terms: dark patterns, dark nudges, sludge, and targeted advertising. As a starting point we looked to the definitions used in highly cited academic papers. Building on commonalities we developed definitions the investing platform context. For this report:

- **Dark patterns** are defined as user interface choices that manipulate, steer, or deceive users into making decisions that benefit the firm but may not align with users' best interests or personal preferences.[3]

- **Dark nudges** are defined as nudges that make it easy for consumers to make choices that decrease their welfare.[4]

- **Sludge** is defined as elements within a user interface that actively impede activities that are in the consumers' best interest, resulting in a reduction of welfare.[5]

- **Targeted advertising** is a form of online advertising. It is defined as a digital marketing practice that uses data about individuals to select and display ads or other forms of commercial content.[6]

With these definitions in hand, we were able to map the relationship between them and the broader categories including dark patterns, dark nudges, sludge, and targeted advertising. Visualized in Figure 1, dark patterns, dark nudges, and sludge are all subsets of Online Choice Architecture. While they are largely distinct from each other, there is overlap between what can be classified as a dark pattern and as dark nudges or sludge (although those latter two categories are mutually exclusive). Prior work by BIT and the OSC focused on the role of gamification, which is also a subset of Online Choice Architecture and has some overlap with dark patterns, in investing platforms.[7]

A defining characteristic of dark patterns, dark nudges, and sludge is that **they undermine investor welfare, interests, and/or preferences**. This requires an understanding of the actions or behaviours that have a negative impact on retail investors, on average. We identified the following key considerations:

- **Active trading:** There is a robust evidence base linking increased trading volume to lower retail investor returns over time,[8] as a result of both the timing of retail investor trades relative to other (e.g., institutional) traders, as well as transaction costs (e.g., commissions, trading fees).

---

[3] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.

[4] Competition and Markets Authority. (2022). Evidence Review of Online Choice Architecture and Consumer and Competition Harm.

[5] Soman, D., Cowen, D., Kannan, N., and Feng, B. (2019). Seeing sludge: Towards a dashboard to help organizations recognize impedance to end-user decisions and action (Research Report Series Behaviourally Informed Organizations Partnership). Research Report Series Behaviourally Informed Organizations Partnership.

[6] Sartor, G., Lagloia, F., and Galli, F. (2021). Regulating targeted and behavioural advertising in digital services How to ensure users' informed consent.

[7] Ontario Securities Commission. (2022). Digital Engagement Practices in Retail Investing: Gamification & other Behavioural Techniques.

[8] Barber, B. M., & Odean, T. (2000). Trading is hazardous to your wealth: The common stock investment performance of individual investors. *The Journal of Finance*, *55*(2), 773-806.

- **Under-diversification:** Diversification is the process of investing in multiple kinds of assets and securities and with varying timing to reduce the specific risk assumed.[9] Under-diversification is costly to most investors.[10]

- **Transaction costs:** Transaction costs such as brokerage commissions, taxes, and fees reduce the returns earned by investors.[11] Transaction costs can be higher either through active trading (see above) or higher fees per trade.

- **Risk profile of securities transactions:** In general, digital assets like crypto assets can be classified as higher risk investments, for reasons including higher volatility. Options trading and trading on margin are also widely understood to be higher risk investment strategies.

The following sections include 11 techniques that are (a) used on at least one platform in our scan, and (b) present a potential risk to investor outcomes. These include seven types of dark patterns, two types of dark nudges, and two forms of sludge:

Dark Patterns	Dark Nudges	Sludge
- Prompts and reminders - Intermediate currency - Ranking - Sensory manipulations - Social norms and interactions - Scarcity claims - Hidden fees / information	- Removal of process steps - Defaults	- Process frictions - Complex language

For each technique, we provide: (1) a definition, (2) summary of current use on digital trading platforms and impact on behaviour, and (3) potential protective measures to mitigate the negative impact on investors.

The section concludes with a discussion of targeted advertising. As this is quite a distinct concept from dark patterns, dark nudges, and sludge, the structure is different. In the targeted advertising subsection, we define and describe types of targeted advertising currently in use, discuss the impact of targeted advertising on consumers, and identify mechanisms to mitigate potential harm. We also provide a more detailed analysis of the use of targeted advertising in the retail investing context.

Dark Patterns

Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions.[12] The following subsections provide more details about the seven dark patterns identified in our

---

[9] Mullins, D. W. (1982). *Does the Capital Asset Pricing Model Work?*. Harvard Business Review.

[10] Goetzmann, W. N., & Kumar, A. (2008). Equity portfolio diversification. *Review of Finance*, *12*(3), 433-463.

[11] Barber, B. M., & Odean, T. (2013). The behavior of individual investors. In *Handbook of the Economics of Finance* (Vol. 2, pp. 1533-1570). Elsevier.

[12] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.

literature and environmental scans. Note that we have anonymized the names of the platforms we examined, as our environmental scan was deliberate and thorough, however, it is not exhaustive of all available platforms.

Prompts and reminders

Definition: Prompts are brief visual, graphic, or auditory stimuli that grab the user's attention to encourage specific behaviours or choices. Reminders are a specific type of prompt that follow up on a previous interaction or engagement. In some instances, prompts and reminders can stimulate behaviour by encouraging more immediate, autonomic decision processes (i.e., activating "System 1" thinking).[13] They can also steer users' decision making by increasing their awareness and / or directing their attention to a certain choice or action.

When this choice or action has negative consequences for the user, prompts and reminders are a **dark pattern**. Prompts and reminders can also be a **dark nudge** if they include links to take action, thereby making it easier, and this action negatively impacts users. This technique can be the vehicle for other dark patterns, like scarcity or popularity claims, likely boosting the efficacy of those dark patterns by making them more salient. Many prompts / reminders do not negatively impact users; they can also be benign or helpful.

Current use on digital trading platforms and impact on behaviour: The majority of platforms examined in our environmental scan use prompts and reminders throughout the user experience. Many of these prompts may benefit the user by helping them follow through on their intentions. For example, we observed prompts to complete the account set-up process, which are most likely to help users execute an intended action and are not a dark pattern. However, other prompts appeared to encourage users to open certain accounts or engage in trading behaviours that may benefit the firms but not investors.

For example, a US trading platform sends push notifications, a form of prompt, to customers when the intraday return of a stock in their portfolio reaches +/- 5%. This type of push notification has been shown to increase the number of retail investor trades by approximately 25% in the minutes following a notification[14] and to exacerbate the disposition effect.[15,16] These prompts can also increase risk taking, with one study showing that trades executed within 24 hours of receiving a push notification bore 19-percentage-point higher leverage.[17] The impact was stronger for male, younger, and less experienced investors. These prompts are a dark pattern when they are not specifically requested by an investor and influence trading volume and risk-taking.

Other apps we reviewed use push notifications to turn users' attention towards specific asset classes, mainly crypto assets. For example, a Canadian trading platform sends out push notifications to alert users of new crypto assets that have become available on the app, even if they've never previously purchased any crypto assets (see Figure 2 for an example). This

---

[13] Gawronski, B., and Creighton, L. A. (2013). Dual process theories. Oxford University Press.

[14] Moss, A. (2022). How Do Brokerages' Digital Engagement Practices Affect Retail Investor Information Processing and Trading?. Working Paper.

[15] The tendency to sell stocks that have recently increased in value and hold stocks that have recently decreased in value

[16] Glaze, J. (2022). Fast-Thinking Attention and the Disposition Effect. *Available at SSRN 4121793*.

[17] Arnold, M., Pelster, M., & Subrahmanyam, M. G. (2022). Attention triggers and investors' risk-taking. *Journal of Financial Economics*, *143*(2), 846-875.

may encourage some investors who do not have a strategy that includes investing in new coins (or crypto more generally) to do so. While some may argue that these prompts simply inform users of new potential investments, the higher risk profile of crypto—combined with the strong incentive of firms to encourage crypto trading—make this a dark pattern.

Figure 2: Example of a prompt (push notification) sent, which promotes the release of a new cryptocurrency available on the platform.

Many apps also use push notifications as a vehicle to present time-limited offers to users. The impact of these types of offers are discussed in the section on Scarcity and Popularity Claims, below.

Protective measures: We did not identify any research regarding protective measures against attention-inducing prompts and reminders. From a theoretical perspective, we believe that making it easy to turn off notifications (e.g., a single click) and salient to do so (e.g., through prominence in the UI or notifications) is likely to help. A stronger approach, employed on some platforms, is to have prompts turned off by default. Investors who do want these notifications could still opt-in.

Intermediate currency

Definition: Intermediate currencies obscure the price of an item by providing it in a currency other than the normal, predominant currency.[18] In general, people are better able to assess prices in their own currency (e.g., CAD for Canadians) and people tend to more accurately estimate the value of a good or service in a familiar currency compared to an unfamiliar one.[19] People spend more money when using "scrip," substitutes for legal tender, often in a form of credit than cash.[20] In the context of investing platforms, the use of intermediate currency can deceive users by presenting important information like fees in crypto assets or foreign currency, which is less familiar to users and requires conversion. The platforms we reviewed did not make conversion easier by embedding a tool in the interface. When a fee is given as a small fraction of a crypto asset, it makes the fee seem less costly, even if the actual value is high because the price of the coin is high. Overall, users are likely to underestimate the cost of investing and may also enter transaction values that are outside their investment strategy when dealing with intermediate currency. In these instances, intermediate currency is a **dark pattern**. When investors face additional cognitive load as a result of unfamiliar numbers or decimal points, or go the extra mile to find and calculate the conversion, the use of an intermediate currency would be **sludge**.

---

[18] Rakovic, I. (2022). *Dark finance: Exploring deceptive design in investment apps* (Master's thesis, NTNU).

[19] Alter, A. L., & Oppenheimer, D. M. (2008). Easy on the mind, easy on the wallet: The roles of familiarity and processing fluency in valuation judgments. *Psychonomic bulletin & review*, *15*(5), 985-990.

[20] Raghubir, P., & Srivastava, J. (2008). Monopoly money: The effect of payment coupling and form on spending behavior. Journal of experimental psychology: Applied, 14(3), 213.

Current use on digital trading platforms and impact on behaviour: Since currency exchange is an inseparable part of working with money internationally, intermediate currencies need to be used for transactions in non-Canadian equities or funds that are not hedged to Canadian dollars.[21],[22] However, when trading foreign securities on Canadian platforms, some platforms provide users clear information about the cost of the trade in CAD. Some provide both the cost of the trade in USD and CAD, while other platforms only provide the cost in USD (Figure 3). This
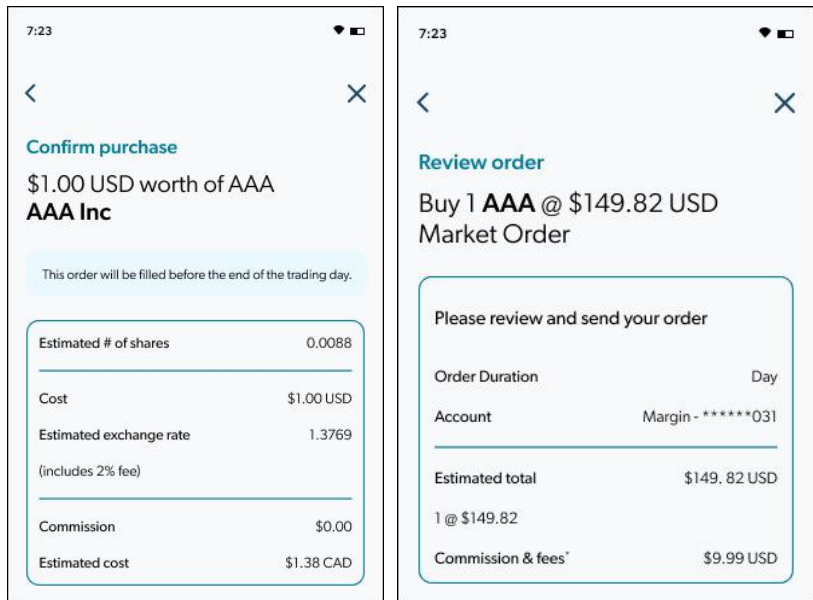

Figure 3: An example of a platform that provides the cost of the trade in both USD and CAD (left), whereas another platform only provides the cost in USD (right).

consideration also applies to fees. For instance, clients of a Canadian trading platform are told they will pay X dollars in fees, without further clarifying that this will be USD for transactions in U.S. dollar accounts.

The use of intermediate currencies is more problematic in crypto trading. Two crypto asset trading platforms examined in our environmental scan state their fees for placing a trade / transferring money out of the account in either the coin being traded or the relevant value-referenced crypto asset (i.e., stablecoin) instead of in CAD (see Figure 4 for an example of a confirmation screen that only shows the transaction in intermediate currency). Others, like one unregulated crypto trading platform we identified, require users to convert fiat currency into crypto assets or value referenced crypto asset (VRCA) when they are depositing funds and then present every subsequent step in the trading process in the crypto asset.

Given their propensity to use digital crypto platforms, younger people may be more susceptible to the negative impact of intermediate currencies. Less experienced investors may also be at higher risk. Research from gaming environments, where microtransactions in a virtual currency

Figure 4: An example of a platform that displays its fee in the relevant cryptocurrency.

---

[21] Note: Users are told it is US$9.95 for trades of US securities in the fee information schedule, as part of the client relationship disclosure documentation provided to clients and available on the app or website.

[22] Rakovic, I. (2022). *Dark finance: Exploring deceptive design in investment apps* (Master's thesis, NTNU).

(a form of intermediate currency) are common, finds that heavy users (e.g., younger consumers) are more vulnerable to overspending in these contexts.[23]

Protective measures: We did not find any research on protective measures against intermediate currency. Protective measures from virtual gaming environments suggest that conversion tables that show the relation between intermediate currencies and real-world prices may increase spending awareness.[24] Providing regular statements of spending activity may also increase cost-related awareness for investors.[25] Stronger approaches could require platforms to provide information on the cost of the trade in CAD, including any fees and the total cost.

Ranking

Definition: Ranking refers to setting the order that options are presented on a user interface in a way that privileges or promotes certain choices.[26] It takes more cognitive (and physical) effort to scroll down a list of items shown on a screen, so items appearing at the top of a list are more likely to be chosen than those later in the list.

Ranking provides users with an easy heuristic to compare items that are ranked, signaling that one item is higher ranked, or better, than another. It steers users by increasing the salience and / or directing attention to certain decisions or choices, even if these are not right for the user or what they would have otherwise chosen. When a ranking is used in this manner on an investing platform, it is a **dark pattern.**

Current use on digital trading platforms: Especially for mobile-first platforms, where only a certain amount of information can be visible to a user at one time, there is no truly "neutral" way to present a series of options, such as a list of stocks. Some platforms present lists of available securities alphabetically, but other apps use other metrics to rank stocks in a way that steers users' attention and choices towards certain stocks. Many platforms prominently feature lists of stocks on their home screens, such as "Top Movers", "Top Losers", and "Most Popular" stocks. The criteria used to generate the ranking are sometimes, but not always given to the user. For example, on one trading platform, we found that the sub-heading "stocks and ETFs with the largest gains in stock price today" accompanies the "Top Gainers" list, but the sub-heading for the 'Recurring Investments' list does not make the ranking mechanism clear (Figure 5).

---

[23] Competition and Markets Authority. (2022). Evidence Review of Online Choice Architecture and Consumer and Competition Harm.

[24] The Committee of Advertising Practice. (2021). Guidance on advertising in-game purchases. https://www.asa.org.uk/static/4028c436-5861-4035- 8d98c148d3c66b7e/Guidance-on-advertising-in-game-purchases.pdf

[25] King, D., and Delfabbro, P. (2018). Internet gaming disorder: Theory, assessment, treatment, and prevention. Academic Press.

[26] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI conference on human factors in computing systems.

Several studies have demonstrated that these types of lists significantly influence investor behaviour. The inclusion of a stock on Robinhood's "Top Movers" list is associated with it being traded 36 more times than the amount that the same stock is traded, even when controlling for overall market activity.[27] These types of stock lists are also significantly associated with increased "herding" behaviour, where retail investor choices are positively correlated with each other (i.e., many people are making the same trades).[28] Herding can negatively impact returns; one study found an average 20-day abnormal return of -4.7% for top stocks purchased each day.[29] Another study
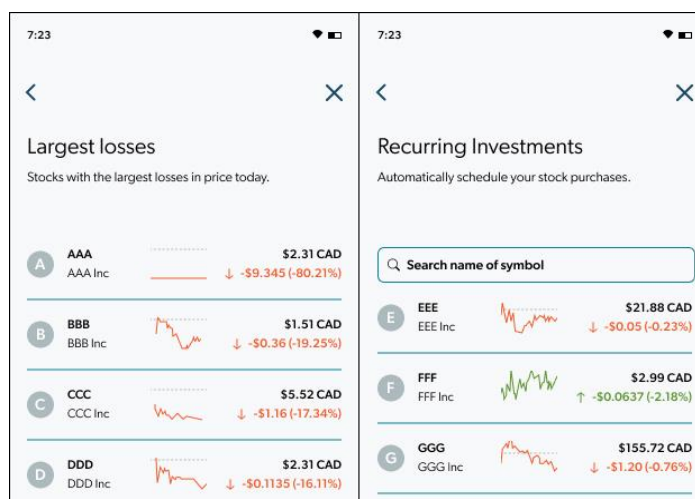

Figure 5: Ranked lists featured on a trading platform. The Top Losers list (left) accompanies an explanation of the ranking criteria, whereas it's unclear how the Recurring Investments list (right) is ranked.

that examined transaction-level data from two German retail banks found that a "Top Movers" list did not impact investor returns.[30] The contrasting results could be a result of different platform interface designs or differences in population. Investors in this study were, on average, 45 years old with nine years of investing experience. Like other DEPs, ranked stock lists may have a more profound effect on younger, less experienced investors, who are the primary market for mobile-first investing apps. In general, ranking effects also tend to be stronger on mobile phones than on personal computers.[31]

Investing platforms also commonly feature "Most Popular" stock lists and lists ranking stocks by their daily trading activity. The impact of this type of list is discussed in the section on Social Norms and Social Interactions, below.

Given the empirical evidence that these types of lists steer users to invest in certain stocks and negatively impact their returns, they are a dark pattern in these instances. Younger, less experienced investors appear to be more susceptible to this technique.

Protective measures: We did not find any research on protective measures against ranking. As a starting point, having platforms explain the criteria used to rank the lists may help investors make more informed decisions. For example, a platform would need to disclose whether lists are based on overall market data (e.g., across TSX trading) or platform-specific data (i.e., a single platform's user base), with the former being less problematic. In addition, lists could be moved to a different section or tab of the platform, so that users need to

---

[27] Nijboer, R. (2021). Retail investing in the information age: an investigation of herd behaviour on Robinhood. (Doctoral dissertation).

[28] ibid.

[29] Barber, B. M., Huang, X., Odean, T., & Schwarz, C. (2022). Attention-induced trading and returns: Evidence from Robinhood users. *The Journal of Finance*, *77*(6), 3141-3190.

[30] Kalda, A., Loos, B., Previtero, A., & Hackethal, A. (2021). *Smart (Phone) Investing? A within Investor-time Analysis of New Technologies and Trading Behavior* (No. w28363). National Bureau of Economic Research.

[31] Ghose, A., Goldfarb, A., and Han, S. P. (2013). How Is the Mobile Internet Different? Search Costs and Local Activities. Information Systems Research, 24(3), 613–631.

actively seek it out rather than being automatically exposed on the home screen. Going further, platforms could disclose the risks of making investment decisions based on the popularity or activity level of an equity. Types of lists (e.g., "Most Popular") that have empirical evidence demonstrating a negative impact on investors (e.g., increased herding activity) could even be banned from platforms, although there may be subsets of users that benefit from them (e.g., experienced traders whose strategy is to take the opposite side of the market direction).

Sensory manipulations

Definition: Sensory manipulations refer to changes to the user interface that focus the user's attention on one thing to distract them from something else. There are a wide range of visual, auditory, and haptic (by touch) manipulations that fall into this category. Visual manipulations are most common and can include the use of colour, size, positioning, or style. Sensory manipulations matter because users often rely on the information that is most salient to make decisions[32]. If the sensory manipulations increase the salience of actions that are not in a user's best interests, they are a **dark pattern.**

Sensory manipulations can also be combined with other techniques (e.g., a prominently placed popularity claim) to influence users, which may increase the effectiveness of the other technique by diverting more attention to it.

Current use on digital trading platforms and impact on behaviour: Sensory manipulations are ubiquitous in digital environments; here we focus on those instances uncovered in our environmental scan that may encourage user actions that are in the platform's best interest but not necessarily the user's. These instances fall into three key categories.

1. Recurring investments: Many platforms use sensory manipulations to promote recurring investments, where users agree to continuously buy a security at a frequency ranging from daily to monthly. The visual prominence of the recurring investment option may distract user attention from the more typical, individual transaction approach. This may reduce diversification by encouraging investment in a single security. This is a risk when the recurring investments are in individual stocks or crypto assets. (Recurring investments to implement a dollar cost averaging approach for a broad-based ETF, for example, would not hurt investor welfare.) In such instances, and when recurring investments are not accompanied by tools to ensure diversification or prevent overcontributions, they are a dark pattern. Users may also incur more fees if they are making more transactions than they would have otherwise.

   Note that recurring security purchases that constitute a dollar cost averaging strategy, as well as recurring *deposits* are not dark patterns. They can be beneficial to investors and in the instance of deposits, may result in increased savings rates.

---

[32] Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *science*, *185*(4157), 1124-1131.

2. Crypto assets: We found that one platform's crypto-focused accounts are hosted within the same platform's main trading app. Given this feature, the platform is able to advertise and draw users' attention to crypto assets, regardless of whether the user has registered to trade crypto. For example, the positioning of a 'learn about crypto' button as a default option through position and colouring immediately after a user makes a deposit in their account represents a visual sensory manipulation (Figure 6).

Similarly, when we reviewed the same platform, crypto assets featured prominently on the 'Discover' page of the app as 'Trending'. The homepage also drew users' attention toward crypto-related actions, with the home screen displaying an advertisement for the platform's staking feature. This feature allows users to lock up their crypto assets to receive rewards - a complex process in which the platform charges a substantial fee (about 30%) to users.

Figure 6: An example of how once a user funds their account, they are steered towards learning more about crypto.

Given trading and staking digital assets is higher risk, steering users attention to such features *before* a user even registers for a crypto account is a dark pattern.
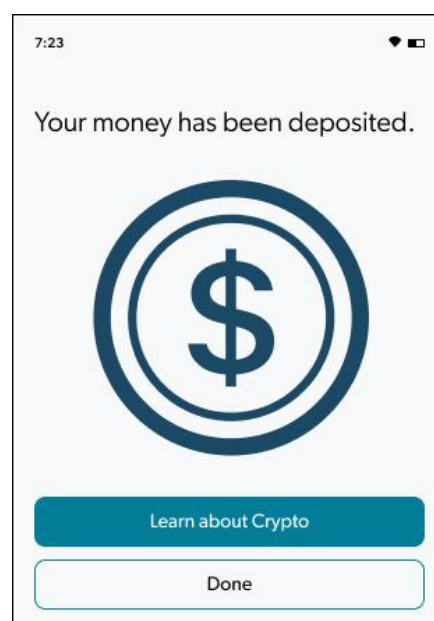
Fees: Visual manipulation can hide certain information by placing it in an obscure part of the page, while using colours and size to make other information more salient. For example, the information page about one platform's 'Advanced' subscription uses a table with prominent red text to highlight the percentage FX fees saved by upgrading to the subscription (Figure 7). From the table, it appears that you pay 0% FX fees on U.S. trades with a Plus membership ($10 / month). The information detailing that you still pay 1.5% FX fees when converting your funds between CAD and USD is less prominently featured on the page. This makes the Plus option appear more attractive, and for those who would not benefit from it, a dark pattern. **Protective measures:** There is a lack of evidence examining protective measures against sensory manipulations. However, some specific actions could be taken like restricting the promotion of securities outside those available within one's current trading account (e.g., not promoting crypto assets to users that do not have a crypto account).

Figure 7: An example of how users' attention is steered towards the 2% difference between a platform's Standard and Advanced plans, and away from the small print.

Social norms and social interactions

Definition: Social norms and interactions refer to two related sets of techniques that leverage how people look to the behaviour of others for cues on their own choices. In the investing platform context, social norms refer to descriptions of how others are investing,

while social interactions refer to how users are prompted to engage with their social networks.

Both social norms and interactions are **dark patterns** because they are designed to *steer* users or potential users toward certain choices (e.g., opening an account, investing in a certain asset).

Current use on digital trading platforms and impact on behaviour: Some platforms use social interactions to encourage users to share activities with their social networks. For example, we found that one crypto platform encourages users to share their transaction after completing a trade (Figure 8). Such action may be detrimental to both users viewing the image and the user posting it. The user sharing the image may serve as an influential messenger for their peers, steering those users' decisions towards actions that may not be aligned with their best interests. Upward social comparison (comparing oneself to "better" peers) has been shown to induce risky trading behaviour, as well as increase trading activity.[33] This type of social interaction also likely increases the disposition effect[34] for the user sharing the investment; they may hold onto losing investments for longer periods of time despite mounting losses to "save face."[35] Overall, we believe that social interactions related to completed trades are a **dark pattern**, but this is primarily a theoretical argument as our literature review did not indicate
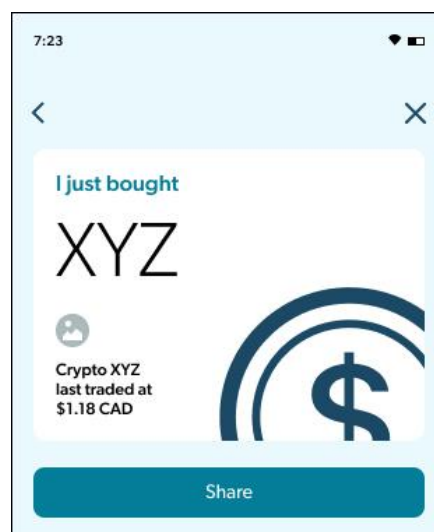

Figure 8: In one example, once a user buys a coin on the platform, they are encouraged to share an image with the coin and its last trading price on their social media feed.

any empirical studies on the issue. More research is needed to understand the influence of social interactions on investing behaviour, particularly within the current context of social media.

Several platforms we reviewed all leverage social norms through "Most Popular" lists that highlight investment options based on their popularity in other users' trading activity. These lists do not present the most traded securities at a market level, but rather within the platforms themselves. This provides an incomplete and often skewed picture of actual trading activity by, for example, excluding the trades of institutional investors.

---

[33] Andraszewicz, S., Kaszás, D., Zeisberger, S., & Hölscher, C. (2022). The influence of upward social comparison on retail trading behavior.

[34] The disposition effect refers to the general tendency of investors to sell securities that have increased in value and hold on to securities that have gone down in value.

[35] Chaudhry, S., & Kulkarni, C. (2021, June). Design Patterns of Investing Apps and Their Effects on Investing Behaviors. In *Designing Interactive Systems Conference 2021* (pp. 777-788).

Robinhood's "100 Most Popular" stock list feature has been shown to significantly impact investors' trading decisions. For example, entries into the list (the 100 stocks most widely held by Robinhood users) are five to seven times more likely to be purchased in the days following their addition to the list.[36] Another platform uses other, more subtle references to popularity to draw users' attention towards certain securities, such as listing crypto under 'trending categories', implying other users are interested in these securities. We found that one unregistered crypto trading platform, has also incorporated popularity indicators into the "Market Stats" it displays. Along with some traditional indicators like market cap and volume, users are shown the asset's popularity ranking[37] and trading activity[38] (Figure 9). Steering the attention of users toward select assets (i.e., the most popular ones) promotes "herding" on investment choices, which in turn has a detrimental impact on retail investor returns. For example, the top 0.5% of stocks bought by Robinhood users each day experiences negative average returns of approximately 5% over the next month, with more extreme herding events being followed by negative average returns closer to 20%.[39] Features that draw users' attention towards the popularity of an asset therefore constitute a dark pattern.

Protective measures: While many trading platforms incorporate social interactions within apps, we see limited evidence on protective measures against such features. Social features like prompts to "post" trades could be restricted. The use of social norms through "Most Popular" lists could be restricted, require a disclosure of how exactly it is determined, or be required to use market-wide rather than platform-specific data.

Figure 9: One unregistered crypto trading platform includes Popularity and Trading activity as key market stats

Scarcity claims

Definition: Scarcity claims are statements that a product or service will not be available for long due to limited supply, pending price increases, or other factors. They pressure consumers to buy products or services immediately, limiting further consideration or due diligence, by playing to human beings' loss aversion and scarcity bias.[40] Scarcity claims are commonly used in digital marketing. For example, a countdown timer will prominently display that an offer or deal is about to expire after a fixed time period (e.g., "5 hours, 28 minutes left!" or "Final day to save!") putting pressure on users to act quickly. This urgency can also be created without providing a specific deadline. For example, time-limited offers may

---

[36] Stein, R. (2020). The Top 5 Predictable Effects of New Entries in Robinhood's '100 Most Popular' List. *Available at SSRN 3694588*

[37] The ranking is based on the relative market cap of tradable assets on the platform

[38] This data point is based on the percentage of the platform's customers who increased or decreased their net position in the coin over the past 24 hours through trading

[39] Barber, B. M., Huang, X., Odean, T., & Schwarz, C. (2022). Attention-induced trading and returns: Evidence from Robinhood users. *The Journal of Finance*, 77(6), 3141-3190.

[40] Kahneman, D., & Tversky, A. (1977). Prospect Theory. An Analysis of Decision Making Under Risk. doi:10.21236/ada045771

indicate that an offer or deal will expire "soon." Platforms may also intentionally withhold a deadline to create pressure and uncertainty in users' minds (who might think that this offer will end at any moment). This may push them to accept an offer without carefully considering it, based on a fear that they might lose the opportunity.[41]

Scarcity claims may not always be harmful, and in some instances might help consumers make decisions based on availability of a particular product. However, they can be designed and deployed in ways that create a false sense of urgency and limit deliberate reflection. In these instances, scarcity claims are a **dark pattern**.

Note that we are not considering patently *false* scarcity claims in this section, as those are not dark patterns - they are outright fraud. As an example, in 2022, the New York Attorney General charged a well-known online travel agency for deceptive marketing practices that used false scarcity claims to generate urgency.[42]

Current use on digital trading platforms and impact on behaviour: Our environmental scan shows platforms most commonly leveraging scarcity claims in the form of time-limited offers. Many trading platforms feature introductory offers, where users can receive "bonus cash" for registering and/or funding a trading account. These are time bound - users are told

they have a certain number of days before the offer will expire. Figure 10 shows a time-limited offer presented to the user as an in-app notification that encourages a deposit or account transfer by a specific date (Dec 4th) to earn bonus cash. These offers are made so consistently that the deadline is somewhat misleading.

Even after depositing funds, users continue to receive time-limited offers to incentivize additional deposits by a certain date. These promotional periods are often linked to special "days" (e.g., "Earn up to $5,000 this Black Friday" etc.) and attempt to generate enthusiasm for potential winnings. We found that one platform would regularly communicate special offers that require immediate action (e.g., "Deposit now for a chance to win cash"). While these deadlines are technically accurate, the urgency may encourage users to contribute more to an account than they otherwise would, especially in light of how commonly such offers are made available.

Figure 10: One platform presents time-limited offers to users upon registration

---

[41] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.

[42] Kelleher, Rowan. (2022). New York AG Slaps Online Travel Company with $2.6 Million Fine, Citing Predatory Behavior. Forbes.

Platforms will also use scarcity claims in combination with other techniques, increasing the influence they may have on user behaviour. For example, we found that one platform combines scarcity claims with prompts (also discussed in the 'Prompts and Reminders' section). They will use push notifications or email communications as a vehicle to present movements in the market, making them more salient to users and generating a sense of urgency (Figure 11).

Another platform may be encouraging users to trade more by highlighting the number of free trades they have remaining before that total resets the following year (Figure 12). Users may think they should "use up" those trades to get as much value as possible from the offer, triggering loss aversion.

Protective measures: We see limited evidence on protective measures against scarcity claims. However, regulations around the type and level of pressure a platform can put on its users could be explored (e.g., platforms could be restricted from using push notifications for offers that expire in less than a day, or whatever amount of time is required for meaningful consideration and due diligence).

Figure 12: One platform presents referral bonuses as a time-limited offer, increasing urgency for users.

Hidden fees / information

Definition: Information about fees or other important platform features like privacy protections can be "hidden" through outright omission, delayed disclosure (i.e., disclosure that is later in the customer journey than when it would be most valuable), or complex language, among other means. For example, potential customers may not receive critical information prior to registering for an account or making a transaction. Users might only learn of additional costs or fees at the final stage of completing a transaction, a specific tactic known as "drip pricing." At this point, users may have been drawn in by a lower price, made a selection, provided personal information, and consented to terms and conditions. This technique activates a user's sunk cost fallacy bias: at the final stage of a transaction, users will likely feel invested / more likely to accept additional charges, in order to not waste their expended effort.[43] This technique deceives users and is a **dark pattern** when users do not find the hidden information. If the user ultimately finds the information (e.g., by searching for fee schedules on separate web pages, etc.), this practice would be **sludge** instead.

Figure 11: One platform gives users X number of free trades within a calendar year, creating pressure to use them before they run out.

Current use on digital trading platforms and impact on behaviour: Our environmental scan shows that hidden fees / information occur throughout the user experience:

---

[43] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.

1. **When registering:** Platforms often hide or obscure important information from users when they are registering for an account. For example, Robinhood offered commission-free trading without mentioning other costs of investing akin to commissions in their impact on investors, and were charged by the U.S. Securities and Exchange Commission for offering commission-free trading, but executing at prices higher compared to other brokers.[44]

    Similarly, some platforms will only partially disclose costs incurred by users. For example, when completing cross-border transactions, platforms will disclose a currency conversion fee, but not mention an additional mark-up that is added to the exchange rate.

    Platforms may also provide fee information in dense, complex agreement documents (e.g., terms and conditions, privacy policies). Often, users will need to exit the registration process and open separate PDFs or webpages to access this information. In one instance, a "Fee Schedule" is referenced within one platform's terms and conditions document - however, no details or links are provided to access this document. To learn more, a user would need to navigate or search for this document on the website themselves. Another platform describes its fees for currency exchange in basis points (e.g., "there is a fee of 150 basis points when you need to exchange currency"), which is likely less intuitive for users than a percentage fee.

    After a user has registered and begins using a platform, it may be difficult to find this information again. For example, we found that if a user on one platform searches for fee information in the Account Documents section of the platform, they are told they can request a fee schedule be emailed to them. This additional step makes it difficult to access this information when a user needs it, and qualifies as sludge.

2. **When considering targeted / time-limited offers or promotions:** Platforms present users with time-limited offers, promising potentially large savings or bonuses if they take a certain action. However, the specific terms of the offer are sometimes hidden unless a user searches for them, often by navigating to a different webpage or clicking on the conditions. What a user will receive, in reality, may often be quite different than what was promised up front. For example, we found that one platform advertises a large bonus if a user refers their friends (up to several thousand dollars) - in reality, 99% of users will receive less than $50. This information is not mentioned in the offer but can be found if a user searches for it in the platform's help centre.

3. **When trading:** Our environmental scan revealed three ways that platforms hide information about costs in the trading process: low salience disclosure, drip pricing, and limited disclosure of crypto asset spreads. Intermediate currency, discussed in a dedicated section above, is also a form of hidden information that is relevant when trading.

    One crypto-trading platform only discloses its operations fee if users access a "tooltip" (i.e., clicking on a 'question mark' symbol next to the transaction amount). This is an

---

[44] U.S. Securities and Exchange Commission. (2020). SEC Charges Robinhood Financial With Misleading Customers About Revenue Sources and Failing to Satisfy Duty of Best Execution.

example of a low salience fee disclosure. Other examples include disclosing fees in small print.

Drip pricing is a practice where fees are only disclosed late in the customer journey, after the customer has taken a number of steps toward completing the transaction. Several of the platforms we reviewed only disclose their fees clearly in CAD at the "trading confirmation" screen, the last step before a trade is executed - prior to this, they may be expressed in less clear ways, such as percentages. This is problematic because of sunk cost bias - people already feel like they are committed to the transaction because of the steps they have taken. They are less likely to consider the fees than they would be if those fees were disclosed at the outset of the trading process, on the main trading screens.

Most crypto asset trading platforms we reviewed do not clearly explain the "spread" that they offer between the price they buy and sell the same coin at. While this spread is not necessarily a fee taken by the platform, it does constitute part of the cost of investing, and would be beneficial for investors to clearly understand that the platform is embedding a fee in the spread. This is particularly true as our environmental scan indicated that different platforms have different spreads on the same coin.

Protective measures: While many trading platforms employ the use of hidden fees within their apps, we did not find empirical evidence regarding protective measures. Platforms could be asked to present all relevant, common fees and commissions as part of the core user journey when setting up their account and considering a trade. They could be required to present fees in local currency alongside other foreign or crypto assets on the trade confirmation screen, a total amount denoted in the local / domestic currency, clearly demarcating fees, and other costs of investing, should be implemented.

The deceptive nature of hidden fees has resulted in regulatory enforcement in the past. Under section 5 of the Federal Trade Commission (FTC) Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce," the FTC has charged companies for deceiving consumers by not fully disclosing hidden fees. One company was charged with using prominent visuals to falsely promise "no hidden fees" when disbursing loans, when in reality, the company deducted thousands of dollars in hidden fees.[45] In 2019, the Competition Bureau of Canada penalized two large ticket sellers for drip pricing - consumers were charged additional mandatory fees during the later stages of the purchasing process.[46] We discuss this example further in the Regulatory Review section, below.

Dark Nudges

Dark nudges are changes to choice architecture that make it easier for consumers to make choices that decrease their welfare.[47] Our environmental scan and literature review indicated two forms of dark nudges that were prevalent on investing platforms and created a risk of negative impact on investor outcomes: the removal of process steps and use of defaults.

---

[45] Federal Trade Commission. (2022). Bringing Dark Patterns to Light.

[46] Government of Canada. (2022). Deceptive marketing practices - Cases and outcomes.

[47] Competition and Markets Authority. (2022). Evidence Review of Online Choice Architecture and Consumer and Competition Harm.

Removal of process steps

Definition: Practices that make it easier for users to make inadvertent or ill-considered decisions by removing the requirement for one or more actions (e.g., confirmations). While simplifying the overall user experience and reducing points of friction can save users' time and increase engagement, it can also make undesirable behaviours *too easy* to take and remove opportunities for reflection. In these instances, users may make decisions that are not aligned with their preferences, especially when they are in "hot" visceral states (e.g., when they are strongly influenced by exhaustion, loss aversion, or other strong emotions).[48,49] In these instances, the removal of process steps is a **dark nudge**.

Current use on digital trading platforms and impact on behaviour: Many trading platforms feature sleek mobile app interfaces that create an experience that is easily navigable, interactive, and intuitive to users.[50] This is largely positive for investors. However, the introduction of "positive friction" into the user experience can also benefit the user in specific instances. For example, the majority of platforms examined in our environmental scan feature a confirmation page before a user submits their order. These pages give an overview of the trade before the user confirms it, 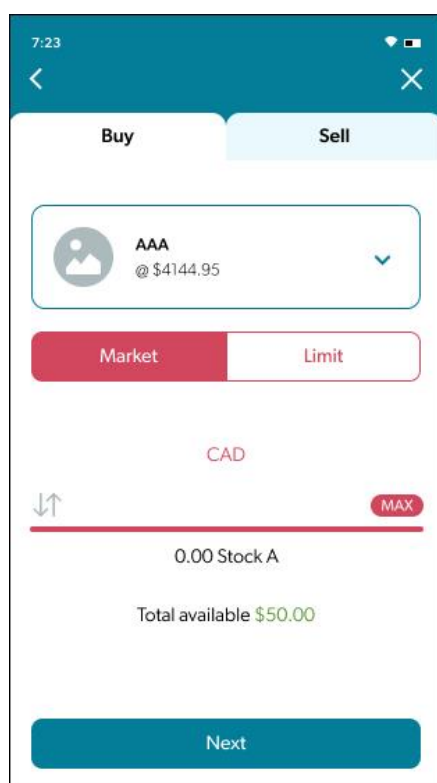providing an opportunity for the user to reflect before making a trade. However, two of the platforms we examined do not include this step, allowing "one click" trading. While another platform has a confirmation screen, it allows users to confirm with a swipe-up gesture instead of the clicking of a button, a different approach to reducing friction in trading.[51]

Three of the platforms examined in our environmental scan also make it easy for users to invest the full value of their cash on hand in a single trade. They feature a salient 'max' button on the 'buy' page where a user enters the value of a crypto asset they would like to purchase (see Figure 13). We hypothesize that the availability and prominence of this button encourages users to adopt this approach at a higher rate than they otherwise would, likely reducing portfolio diversification.

The set-up of some investing platforms also reduces friction for investors to buy crypto assets in particular. In two of the platforms we reviewed, users can trade both types of securities within the same app. While the actual trading of crypto is done through a separate account (that the user must sign up for in addition to the trading account), the accounts are housed within the same

Figure 13: One platform's Buy page features a 'Max' button to use all available funds to place the trade

---

[48] Birner, K. (2015). One click to empowerment?: Opportunities and challenges for labour in the global value chain of e-commerce. International Journal of Labour Research, 7(1/2), 55.

[49] Loewenstein, G. (2005). Hot-cold empathy gaps and medical decision making. Health Psychology, 24(4S), S49.

[50] Tan, G. K. S. (2021). Democratizing finance with Robinhood: Financial infrastructure, interface design and platform capitalism. *Environment and Planning A: Economy and Space*, *53*(8), 1862-1878.

[51] Tan, G. K. S. (2021). Democratizing finance with Robinhood: Financial infrastructure, interface design and platform capitalism. *Environment and Planning A: Economy and Space*, *53*(8), 1862-1878.

platform / app, making it easier for users to trade both stocks and crypto assets without having to leave the app or log in and out. One of the platforms also show their users advertisements for crypto trading, regardless of whether they actually hold a crypto account (discussed in Sensory Manipulations). They will also see coins and other securities displayed on the same screen (e.g., when browsing "Most Popular" lists), which could lead to greater interest in crypto assets through mere exposure. As a result, users whose investment strategy did not involve trading crypto assets may be more likely to engage in this activity.

Some platforms have removed process steps and simplified the interface for making higher risk types of trades (e.g., options), compared to prevailing industry norms. For example, new users can begin trading options on one platform immediately after answering a few simple multiple-choice questions.[52] The user simply needs to self-attest to having investment experience greater than "none", and a risk appetite that is "medium or greater". Complaints have been made against the platform for not adequately enforcing its own minimal policies and procedures to approve users for options trading.[53] These types of trades are more lucrative for the platform, as spreads are higher for riskier and more volatile products like options, meaning high frequency trading firms pay more for them.[54] As a result, inexperienced investors may begin trading these risky products without a good understanding of the inherent risks. A New York Times analysis found that Robinhood customers bought and sold *88 times* as many risky options contracts as Charles Schwab customers, relative to the average account size.[55] Several studies have demonstrated a detrimental effect on investors - the more options a retail investor trades, the more poorly they perform,[56] and the losses incurred on options investments are much larger than those incurred from equity trading.[57]

Protective measures: Re-incorporating friction into processes where it is known that users are making fast decisions (e.g., placing a trade) may help prompt vigilance and thoughtfulness in decision making.[58] For example, the Danish Government introduced a law in 2017 that mandates a 48-hour waiting period before consumers can finalize an application for payday loans to give consumers an extra opportunity to deliberate and avoid making impulsive financial decisions.[59] In an investing context, one-click trading could be disallowed and further process steps could be mandated for users to be able to trade in particularly high-risk ways, like options. This could build on existing process steps - for example, the Canadian Investment Regulatory Organization (CIRO; recently known as New Self-Regulatory Organization of Canada [New SRO]) process includes submitting an application

---

[52] ibid.

[53] Kelleher, D. M., Grimes, J., & Chovil, A. (2022). Securities—Democratizing Equity Markets with and Without Exploitation: Robinhood, Gamestop, Hedge Funds, Gamification, High Frequency Trading, and More. *Western New England Law Review*, *44*(1), 51.

[54] ibid.

[55] ibid.

[56] Li, Y., Zhao, C., & Zhong, Z. K. (2021). Trading behavior of retail investors in derivatives markets: Evidence from Mini options. *Journal of Banking & Finance*, *133*, 106250.

[57] ibid.

[58] Soman, D., Cowen, D., Kannan, N., and Feng, B. (2019). Seeing sludge: Towards a dashboard to help organizations recognize impedance to end-user decisions and action (Research Report Series Behaviourally Informed Organizations Partnership). Research Report Series Behaviourally Informed Organizations Partnership.

[59] Competition and Markets Authority. (2022). Evidence Review of Online Choice Architecture and Consumer and Competition Harm.

to trade options. An additional process step could include testing a retail investor's understanding about options and the risks involved prior to enabling trading.

Defaults

Definition: A default is a preselected setting that automatically takes effect unless users actively change it. Defaults are powerful and sticky, with users tending to stick to them at a high rate across diverse contexts due to inertia[60] and several other factors.[61,62]

Defaults are an inherent element of any platform and can benefit investors. However, they can also shape user behaviour in ways that undermine their intentions and best interests by making that behaviour easier, even automatic. In these cases, they are a **dark nudge**. Because users must take additional steps to change default settings, they are also **sludge**.

Current use on digital trading platforms and impact on behaviour: In our environmental scan, most investing platforms default users into receiving communications when registering for an account and providing their email address and / or phone number. Agreement documents (e.g., terms & conditions, privacy policies) state that when a user provides their personal information, the platform will use it to send marketing communications, or communication about products and services. Users are not given the option to choose whether or not they want to receive this information when registering, but are told they can unsubscribe at any time.
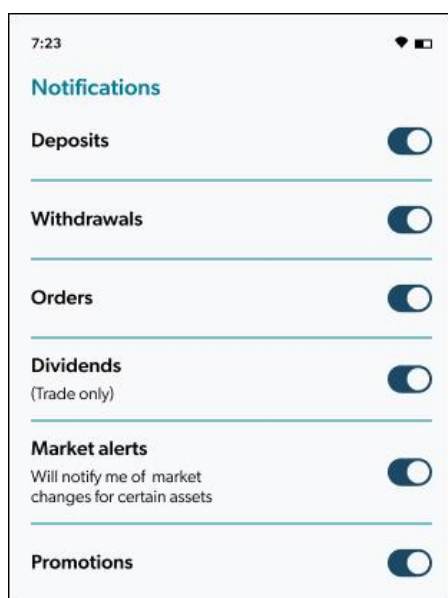
Most platforms also automatically opt users into receiving mobile push notifications. For example, on one platform, when a user signs up, they are defaulted into receiving mobile notifications for deposits, withdrawals, orders, dividends, opportunities to earn cash, market alerts, promos & tips, etc. (Figure 14). The user has the option to toggle off each type of notification in the app settings, but must do so for each individual type of notification. This additional friction can be characterized as sludge.

Similar to *prompts and reminders,* marketing communications and mobile push notifications can impact behaviours by encouraging actions that users might not otherwise take. In some cases, these actions can work against a user's best interest (e.g., if a user is influenced to begin trading crypto assets - a higher risk product). By defaulting users into receiving these types of communications, more investors will be exposed to messaging that they have not actively chosen / does not align with their investment strategy. As a result of the "mere

[60] Johnson, E., Bellman, S., and Lohse, G.L. (2002). Defaults, Framing and Privacy: Why Opting In-Opting Out1. *Marketing Letters* 13, 1 (01 Feb 2002), 5–15.

[61] Dinner, I., Johnson, E. J., Goldstein, D. G. and Liu, K. (2011). Partitioning Default Effects: Why People Choose not to Choose. *Journal of Experimental Psychology: Applied*, 17(4): 332–341.

[62] Jachimowicz, J., Duncan, S., Weber, E., & Johnson, E. (2019). When and why defaults influence decisions: A meta-analysis of default effects. *Behavioural Public Policy, 3*(2), 159-186.

Figure 14: One platform defaults users into receiving email and mobile notifications, which they must turn off one-by-one in app settings.

exposure effect"[63], this increased familiarity may cause users to develop a preference for products or investments they might not otherwise.

In many instances, platforms also default users into allowing the collection and sharing of personal information as part of long, complex privacy policies. Also known as "privacy zuckering," this may cause users to share more information about themselves than intended. For example, we found that one platform's privacy policy states that it collects information that is shared as part of the registration process (e.g., name, street address, telephone number, email address, credit card and other payment information, etc.), as well as through cookies that collect information during and about visits to platforms and other tracking technologies (e.g., pixel tags). The platform also states that the information they collect and use may be shared with third parties such as affiliates, suppliers, or agents.

The average user will not understand the complexity of data collection and sharing and may feel overwhelmed by these privacy policies. Many do not even know their options to influence what data is collected or shared. Defaulting users into these policies makes it more likely their information will be shared when they might not feel comfortable.

Protective measures: While many trading platforms incorporate defaults within apps, we found limited evidence on protective measures against them. From a theoretical perspective, users should be given an opportunity to opt-in to privacy settings, or marketing communications or push notifications that interest them - otherwise platforms should ensure that settings, such as sharing user information with third parties, are turned off by default.

This is especially critical around users' privacy and data sharing considerations. It is important that consumers receive privacy protection by default - with options to adjust / opt-in according to their own preferences. Platforms should also be more transparent about sharing privacy policies, instead of burying them in long, complex privacy policies that users may not read or understand.

While investing-specific measures do not yet exist, the United States Federal Trade Commission (FTC), European Union (EU), and other regulators have taken action to protect consumers from harmful privacy and data sharing policies more broadly. Under the Federal Trade Commission Act, the FTC has the authority to prevent unfair or deceptive trade practices.[64] It has filed cases against companies that violate data sharing stipulations (e.g., a TV manufacturer that enabled a default setting to collect and share unaware consumers' television viewing activities with third parties).[65]

---

[63] An effect whereby people's tendency to show an increased preference or liking for something the more that they are exposed to it.
[64] Federal Trade Commission. (2022). Bringing Dark Patterns to Light.
[65] ibid.

The European Union's General Data Protection Regulation (GDPR) has also created a robust regulatory framework to protect consumers' data sharing and privacy rights (see more details in the Regulatory Review section below).[66] Under the GDPR, companies are required to obtain informed consent that entails the provision of "clear, accurate, and unambiguous information" prior to obtaining consent. Companies must ensure that consumers are able to make informed decisions, understand what they are agreeing to, and actively agree through a motion or declaration. Companies are also required to build privacy-by-default stipulations into their product development processes.[67] This would ensure that only data strictly necessary for a specific purpose are processed by default (without the intervention of the user).[68]

Canada has also started updating privacy and data protection laws. The federal government has proposed the Digital Charter Implementation Act (Bill C-27), in order to modernize the framework for the protection of personal information in the private sector and introduce new rules for the development and deployment of artificial intelligence (AI).[69] This legislation aims to protect the privacy of Canadians by (1) increasing control and transparency when sharing personal information; (2) giving Canadians freedom to move their information in a secure manner, and (3) ensuring that information is destroyed when consent is withdrawn.

While privacy legislation is being considered, best practices that support greater transparency and consumer understanding around informed and active consent, could be encouraged. For example, the Behavioural Insights Team, in collaboration with the U.K. Department for Business, Energy, and Industrial Strategy, has developed an evidence-based 'Terms and Conditions' best practice guide. This resource encourages businesses to prioritize consumer comprehension in their product development stage. It also provides a list of 18 proven techniques intended to help businesses simplify the detail of terms, resulting in adequately informed consumers.[70] We believe these techniques would help investing platforms enable users to make more informed decisions about their privacy.

Sludge

Sludge is defined as elements within a user interface design that actively impede activities that are in the consumers' best interest, resulting in a reduction of welfare.[71] Sludge differs from dark patterns and dark nudges, as sludge impedes users in completing at an action desired by users, whereas dark patterns and dark nudges generally steer users towards a particular action (often undesired by users). Our environmental scan and literature review identified two forms of sludge that are prevalent on investing platforms and create a risk of negative impact on investor outcomes.

---

[66] Adeyoju, A. (2022). Privacy Dark Patterns: A Case for Regulatory Reform in Canada.

[67] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[68] European Data Protection Supervisor. (2022). Privacy by Default.

[69] Government of Canada. (2022). Canada's Digital Charter: Trust in a digital world.

[70] Behavioural Insights Team. (2019). Best Practice Guide - Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses.

[71] Soman, D., Cowen, D., Kanna, N., Feng, B. (2019). Seeing Sludge: Towards a Dashboard to Help Organizations Recognize Impedance to End-User Decisions and Action. Behaviourally Informed Organizations Partnership Research Report Series.

Process frictions

Definition: People tend to procrastinate or avoid tasks when they are deemed challenging, tedious, or boring. Sludge plays to this tendency by creating 'psychological fences' that impede an individual's ability to get things done.[72]

Friction is not always harmful to consumers; as discussed in the previous section, friction can be positive when it helps the consumer fully consider their decision. However, when it has a negative influence on users, this friction is called sludge. Firms will sometimes use sludge intentionally and impede consumers from acting in their best interest. The most common example of sludge is how much harder most companies make it to cancel a subscription than it is to subscribe in the first place.

Current use on digital trading platforms and impact on behaviour: In our environmental scan, sludge is prevalent on both self-directed investing and regulated / unregulated crypto platforms when users try to withdraw or transfer money from their account, or try to close their account. Across all platforms, users are required to complete complicated steps / processes (e.g., fill out a form then wait for a representative to be in touch), contact representatives directly (e.g., call or email a representative with a formal close request), transfer any remaining balance themselves, and/or pay fees. This type of sludge, sometimes referred to as 'roach motel', tries to maximize user retention by making it harder for users to exit. By adding friction to these processes, platforms may hope that their users will give up on the desired action. Specific examples include:

- **Withdrawing or transferring funds:** Users will often need to navigate complicated processes and take multiple steps when trying to withdraw or transfer from their accounts. On platforms some platforms (see Figure 15 for an example), a user needs to put in a formal withdrawal request, which can take days to process. The

Cyptocurrency	Minimum Withdrawal	Withdrawal Mining Fee
Crypto X (XYZ)	0.3 XYZ	0.03 XYZ
Crypto Y (YZX)	3 YZX	0.3 YZX
Crypto Z (ZXY)	30 ZXY	3 ZXY

Figure 15: One platform presents different withdrawal requirements depending on the cryptocurrency of interest.

whole process of transferring an account can take 4-6 weeks at times, a stark contrast to the minutes it takes to create an account and transfer funds into it. During this period, a user may not have access to be able to transact on their account, making it challenging to respond to changes in the market and/or preventing potential losses.

Users may also incur fees when trying to make withdrawals or transfer accounts, which may disincentivize or reduce the likelihood of them completing the action. One platform lists the different fees a user will need to pay on its website, depending on the action a user takes - for example, CAD electronic fund transfers are free, wire

---

[72] Soman, D., Cowen, D., Kanna, N., Feng, B. (2019). Seeing Sludge: Towards a Dashboard to Help Organizations Recognize Impedance to End-User Decisions and Action. Behaviourally Informed Organizations Partnership Research Report Series.

transfers may cost up to $X, and transferring out of an account can cost $Y. This can serve as friction, as it is another cost that a user must consider before they proceed.

These additional steps and considerations that a user must navigate directly contrast the ease with which users can create accounts or deposit funds. Such processes can feel "automatic" and only take a few minutes to complete, as opposed to the manual, often costly process to transfer or withdraw funds from one's account.

- **Account closing:** On one of the platforms, when users attempt to close their account, they are told they will need to leave the app to submit a request. Once taken to the website, users are required to provide login details again, then asked to complete a request form and wait to be contacted by a customer representative (2-3 business days). From a visual scan of this web page, there is no form that users can fill out. At this point, a user may need to call customer service to close their account. In addition, no information on account closures is provided on the platform's website, including within the Help and FAQ sections.[73] On another platform, users are told to call the platform and speak with an Investment Representative. A user is unable to close the account themselves. We did not attempt this as part of our environmental scan so we cannot determine how cumbersome a process is involved in practice.

- **Account transfer:** Users who want to transfer their accounts, or move funds / securities to a new platform, have to navigate the process between their existing and new provider. The transfer is generally managed by the receiving (new) institution, who may also pay any transfer fees on behalf of the user. Fees vary across institutions - while one platform does not charge any transfer fees, another will charge north of $100 for a full transfer and a smaller amount for a partial transfer. As a result, users do not experience much sludge - a contrast to other types of withdrawals and transfers (see above). However, this process can still take a few weeks to complete, during which a customer does not have access to their account. While crypto can be transferred, completing such a transaction can be complex. For example, users have to be careful inputting transfer details; incorrect information can result in losing one's assets permanently.

Protective measures: While many trading platforms have incorporated sludge within apps, we found limited empirical evidence regarding protective measures. More generally, regulators are taking action to monitor, minimize, and even stop practices that encourage sludge.[74] In 2020, the FTC filed a complaint against an online learning company that was blocking consumers' cancellation attempts. According to the FTC, this company enrolled consumers into 30-day free trials or into 6- or 12-month memberships and, despite promising "Easy Cancellation," many consumers could not cancel even after repeated attempts at calling, emailing, and contacting customer support via an online form.[75]

Leveraging principles from previous cases, platforms could be required to make canceling an account as simple as creating one (i.e., platforms should give users the same options for cancelling accounts that they offer for creating one). As of March 2023, the FTC has formally

---

[73] The hidden information here could be considered a dark pattern as well.

[74] Federal Trade Commission. (2022). Bringing Dark Patterns to Light.

[75] Federal Trade Commission. (2020). FTC Complaint: FTC v. Age of Learning, Inc., also d/b/a ABCmouse and ABCmouse.com, Case No. 2:20-cv07996.

proposed a "click to cancel" rule that requires sellers to "make it as easy for consumers to cancel their enrollment as it was to sign up."[76] This is part of the FTC's ongoing review of its 1973 Negative Option Rule, used to combat unfair or deceptive practices related to subscriptions, memberships, and other recurring-payment programs.

Complex language

Definition: The use of technical, overly complex (e.g., 'legalese'), or lengthy language to confuse or distract the user. Often seen in license agreements, terms and conditions, and privacy statements, this technique can discourage users from reading the given information and obscure what a user might be agreeing to. Language complexity influences how information is processed. Complex language tends to be weighed less heavily and perceived as less valid than easy-to-process information.[77-78]

An empirical investigation of privacy policy / terms of service reading behaviour found that a typical privacy policy can take ~30 minutes to read; terms of service can take ~15 minutes.[79] This information overload is often exacerbated by the use of highly technical, legal terminology that users may not be familiar with. As a result, most users simply agree to these policies without reading them; and those who do read them only spend 73 seconds reviewing them, on average, before agreeing.[80]

Because complex language requires users to spend significant time and mental bandwidth understanding important information, it is primarily classified as sludge. However, if complex information is presented to users with an intent to deceive or obscure (e.g., burying privacy implications intentionally so that users agree without understanding them) it can also be a dark pattern. The use of complex language is particularly harmful because license agreements contain important information (e.g., fee structures, data sharing policies) that investors should understand before agreeing to sign up.

Current use on digital trading platforms and impact on behaviour: In our environmental scan, we see that all trading platforms present users with multiple, lengthy, complex legal documents when they are registering for accounts. These documents present important information to users about the terms and conditions they are agreeing to, privacy implications and how their data is being shared, fee schedules and other disclosures.

Agreements can be even more complex when signing up for crypto asset accounts, recognizing the higher risk profile of such products and government regulation on informing investors of these risks. Users are asked to sign multiple agreements which can range from 30 to 60+ pages.

In our audit of three crypto asset trading platforms, we use the Flesch-Kincaid readability formula to assess the approximate reading grade level of each of their agreements (including

---

[76] Federal Trade Commission. (2023). Federal Trade Commission Proposes Rule Provision Making it Easier for Consumers to "Click to Cancel" Recurring Subscriptions and Memberships

[77] Reber, R., and Schwarz, N. (1999). Effects of Perceptual Fluency on Judgments of Truth. Consciousness and Cognition, 8(3), 338–342.

[78] Shah, A. K., and Oppenheimer, D. M. (2007). Easy does it: The role of fluency in cue weighting.

[79] Obar, J., and Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, *Information, Communication & Society,* 23:1, 128-147.

[80] ibid.

terms and conditions and privacy policies). We find that the readability of these documents is recorded at a reading level of grades 12-15 or at a university / college level.[81] For reference, accessibility and copyrighting guidance usually recommends that documents for the public are written at a grade 8 level, the reading level of an average individual in Canada and the United States[82].

Protective measures: While many trading platforms have incorporated complex language within their documents, we found limited evidence on protective measures against such features.

Wherever possible, trading platforms could simplify information that may have significant implications on user welfare (for example, types of products available, fee disclosure, privacy policies, etc.). However, there may be considerations if products or services require specialized or technical language, or if simplification decreases the accuracy of this information. In these cases, platforms may consider presenting information in two ways - a shortened, simplified format supplemented with a more detailed format that includes technical language.

The FTC requires companies to make consumer choices easy to access and understand. Specifically, "consumers should not … have to look for settings buried in a privacy policy or in a company's terms of service: they should be presented at a time and in a context in which the consumer is making a decision about their data. Any toggle options presented to the consumer should not be ambiguous or confusing, and one option should not be more prominent than another." [83]

The Ontario Securities Commission (OSC) provides guidance on the language used in disclosures, requiring firms to avoid technical terms and generally ensure that disclosures are clear and meaningful. For example, Companion Policy 31-103 notes that "[w]e expect registrants to present disclosure information to clients in a clear and meaningful manner in order to ensure clients understand the information presented. Registrants should ensure that investors can readily understand the information."[84]

Targeted Advertising

Definition and description

Targeting advertising is a form of online advertising. It is defined as *a digital marketing practice that uses data about individuals to select and display ads or other forms of commercial content.*[85]

---

[81] The Flesch-Kincaid Reading Ease Test uses the average length of a sentence and the average number of syllables per word to measure readability.

[82] Richard A, Richard J, Johnston W, Miyasaki J. (2018). Readability of advance directive documentation in Canada: a cross-sectional study. *CMAJ Open.* 6(3):E406-E411.

[83] Federal Trade Commission. (2022). Bringing Dark Patterns to Light.

[84] Ontario Securities Commission. (2022). Unofficial Consolidation: Companion Policy 31-103CP Registration Requirements, Exemptions and Ongoing Registrant Obligations.

[85] Sartor, G., Lagloia, F., and Galli, F. (2021). Regulating targeted and behavioural advertising in digital services How to ensure users' informed consent.

It has been used to augment all three primary types of online advertising (see table below).[86]

Table: Primary Types of Online Advertising (Fourberg, 2021):

Type of Online Advertising	Description
Search Advertising	Linking an ad or a website in a user's search results (e.g., sponsored ad).
Display Advertising	Advertising through visual formats such as: ○ Social media: Advertising shown on social media platforms, often embedded in a user's feed. ○ Video: Advertising shown when users are watching videos, before videos are played or as overlays. ○ Banner: Advertising placed on top of website content, such as pop-ups, overlays, or announcement bars.
Classified Advertising	Advertising displayed as a "slot" on a publisher's website (e.g., sites that promote jobs/recruitment, travel, cars, etc.)

The US Federal Trade Commission has developed a helpful model for understanding the key elements of the targeted advertising ecosystem (Figure 16).[87]

- **Firms** (or Marketers) are groups interested in presenting their offers or products to potential consumers, with a desire to increase sales and revenues. They are willing to pay to have their ads displayed to specific consumers, and may also be interested in increasing awareness and loyalty of their products.
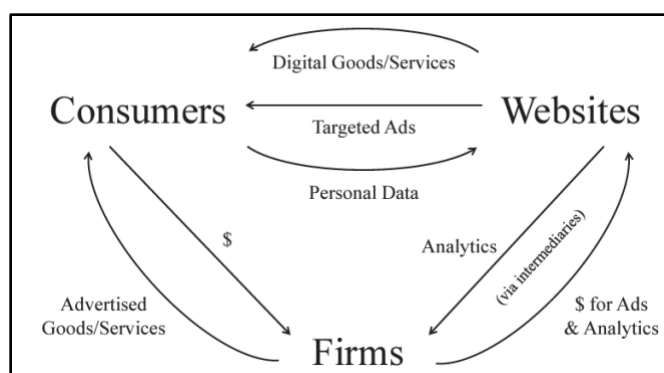

Figure 136: The key elements of the targeted advertising ecosystem

- **Websites** (or Publishers) are groups that provide online content which draw the attention of consumers. Firms will purchase space on a publisher's online interface - this includes large platforms such as e-commerce marketplaces, app stores, search engines, and social media sites. Websites may also collect consumer information using tracking / analytics tools, which can be shared with firms (via intermediaries) for targeting.

- **Advertising Intermediaries** are groups that facilitate connections between demand and supply in advertising spaces (i.e., between firms and websites). This includes data management companies (e.g., platforms, brokers, market research companies)

---

[86] Fourberg, N., Tas, S., Wiewiorra, L., Godlovitch, I., De Streel, A., Jacquem, H., Hill, J., Nunu, M., Bourguigon, C., Florian, J., Ledger, M., and Lognoul, M. (2021). Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice.

[87] Lao, Y. (2020). A Brief Primer on the Economics of Targeted Advertising.

that are able to collect, aggregate, and analyze data. They are then able to build user profiles that include insights and preferences, and sell these to firms. In some instances, firms may have these capabilities available in-house.

● **Consumers**: Groups to which firms are interested in advertising. Once consumers receive targeted information on a website, they may purchase advertised goods and services from firms. They are targeted based on their personal data, including browsing habits, preferences, and demographic characteristics.[88]

There are three main types of data that are used in targeted advertising, contextual, behavioural, and segmented, as detailed in the table below:

Table: Primary Forms of Targeting[89]

Type of Targeting	Description
Contextual	Targeting based on the content of a visited website or search query. For example, a user that searched "cooking" may see advertisements for kitchen appliances. The advertisements shown are determined by the content of the website a user visited, and not by information about the user itself. This is seen most in classified advertising, and sometimes in display advertising (to a lesser extent).
Behavioural[90,91]	Targeting based on a consumer's online behaviour, collected via cookies or other tracking technologies. This involves extensive processing of consumer data, including information that users may share with a platform (e.g., posts, reviews, purchase history, etc.), and technical information about a user (e.g., device, operating system (OS), browser, screen resolution). This is seen most in display and search advertising. Online tracking via cookies is growing at an exponential rate in its reach and sophistication. 85% of the 100 most popular US websites now use third-party cookies to track information about their users.[92] Many firms deploy advanced analytics, machine learning, and cognitive computing technologies to segment individuals, in order to share ads that are most likely to influence them.

---

[88] Lao, Y. (2020). A Brief Primer on the Economics of Targeted Advertising.

[89] Fourberg, N., Tas, S., Wiewiorra, L., Godlovitch, I., De Streel, A., Jacquem, H., Hill, J., Nunu, M., Bourguigon, C., Florian, J., Ledger, M., and Lognoul, M. (2021). Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice.

[90] Yan, J., Liu, N., Wang, G., Zhang, W., Jiang, Y., and Zhen, C. (2009). How much can behavioural targeting help online advertising? World Wide Web Conference, 2009.

[91] Smit, E., Van Noort, G., and Voorveld, Hl. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe.

[92] Sartor, G., Lagloia, F., and Galli, F. (2021). Regulating targeted and behavioural advertising in digital services How to ensure users' informed consent.

Segmented[93]	Targeting based on information a consumer has provided voluntarily (e.g., their name, gender, contact information, when registering a profile or an account). This is often combined with other data to understand user interests.

Contextual advertising - seen as the most basic form of targeted advertising - is most prevalent among firms of different sizes. It is used by over 80% of European businesses that pay for advertising.[94] However, the use of behavioural advertising is growing particularly quickly as a result of its effectiveness - the click-through rate of behavioural advertising can be 5.3 times higher than that for standard advertising.[95] In some instances, firms will combine different targeting techniques together to maximize effectiveness. For example, the complementary nature of a contextual (less personalized) and behavioural (highly personalized) targeting approach has been shown to result in significantly higher engagement and click-through rates.[96] Our research did not indicate which combinations of types of targeting are most influential on consumer behaviour.

Impact on consumers

Targeted advertising increases the effectiveness of marketing spending by bringing tailored content to high-potential consumer audiences.[97] In short, targeted advertising works. There is a broad consensus that targeted advertising is widespread and accelerating,[98] but there is conflicting public data on its extent and impact. Firms and websites are not generally required to disclose the details of their targeted advertising techniques, resulting in a lack of transparency around their practices.

Targeted advertising appears to work most effectively among new users or individuals who are not initially aware that advertising may be targeted or sponsored. This understanding usually shifts over time, with increased exposure to targeted advertising. It also works more among users facing cognitive overload, who either do not have the attention to detect advertising attempts or capacity to search for other alternatives.[99] Curiously, targeted advertising seems to work less well when it is highly personalized. Studies from Tucker (2014) and Aguirre et al. (2015) have demonstrated that very high degrees of personalization can also lead to less engagement.[100,101] Although both studies find that personalized advertising has a greater effect on consumers than non-personalized ads, this effect is

---

[93] European Commission, 2018, Consumer market study on online market segmentation through personalized pricing/offers in the European Union.

[94] European Parliamentary Research Service. (2020)., Digital Service Act: European Added Value Assessment.

[95] ibid.

[96] Fourberg, N., Tas, S., Wiewiorra, L., Godlovitch, I., De Streel, A., Jacquem, H., Hill, J., Nunu, M., Bourguigon, C., Florian, J., Ledger, M., and Lognoul, M. (2021). Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice.

[97] Brahim, N., Lahmandi-Ayed, R., and Laussel, D. (2011). Is targeted advertising always beneficial? International Journal of Industrial Organization 29 (2011) 678–689.

[98] Wall Street Journal.(2021). Advertising Market Keeps Growing Much Faster Than Expected, Forecasters Say.

[99] Fowler, G. (2022). It's not your imagination: Shopping on Amazon has gotten worse. Washington.

[100] Tucker, C. (2014). Social Networks, Personalized Advertising, and Privacy Controls. Journal of Marketing Research Vol. 51, No. 5.

[101] Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K. and Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trustbuilding strategies on online advertisement effectiveness. Journal of Retailing, 91(1), pp. 3449.

lessened if personalization is too precise. This may be attributed to the fact that ads that feel 'too personal' can lead to a process of 'reactance', where consumers deliberately resist ads that they perceive as intrusive.[102]

When the data used in targeted advertising is appropriately obtained - with the informed consent of the consumer - it can be beneficial to consumers. Targeting means that consumers are more likely to see advertisements for products and services they are interested in.

However, users are not always, or even generally, aware of the extent that their data is being used for targeted advertising. When personal data is collected without consent and/or used for purposes that the consumer does not know or approve, consumer privacy is violated.[103] The risk of harm may be greatest in behavioural targeting, when cookies or other tracking technologies are used to collect user data. Users may not understand how cookies work, or unknowingly accept cookie policies when trying to access a website. In some instances, they may not be able to access website content unless they accept its cookies.[104] In addition, firms continue to develop new techniques to track behaviours that consumers are not aware of, making tracking more difficult to stop. Consumer data is also shared across various actors without the consumers' knowledge or consent.[105] Consumers have little agency and limited ways to stop or control the exploitation of their own data.[106]

Dark patterns are frequently used to induce users to provide data that enables targeted advertising.[107] Common dark patterns include default settings, complex information, and sludge. Cookie consent banners may contain sensory manipulations or obstructions that steer users into accepting cookie tracking without fully understanding the implications.

With vulnerable consumers, the concerns extend beyond the nature of the underlying data collection. Details about a consumer, such as their age, health status, financial status, and other personal attributes can be collected and used to target them unfairly, exploiting their vulnerability.[108] Children, people with cognitive limitations, and users new to or unfamiliar with online environments face additional risk given their limited capacity to identify or evaluate targeted ads.[109] They are also at elevated risk from the data collection practices described above.[110]

---

[102] Tucker, C. (2014). Social Networks, Personalized Advertising, and Privacy Controls. Journal of Marketing Research Vol. 51, No. 5.

[103] Pew Research Center. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.

[104] Smit, E., Van Noort, G., and Voorveld, Hl. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe.

[105] Ham, C. (2017). Exploring how consumers cope with online behavioral advertising. International Journal of Advertising, 36 (4):632-658.

[106] Kingaby, H. (2020). AI and Advertising: A Consumer Perspective.

[107] Sartor, G., Lagloia, F., and Galli, F. (2021). Regulating targeted and behavioural advertising in digital services How to ensure users' informed consent.

[108] Center for Digital Democracy (2009).

[109] Blake et al 2015

[110] Alreck, P. and Settle, R., (2007). Consumer reactions to online behavioural tracking and targeting. Journal of Database Marketing & Customer Strategy Management 15(1):11-23

Mitigation options

Privacy experts and scholars have proposed a wide range of mechanisms to mitigate the impact of potentially harmful targeted advertising. These include:

1. Increasing the transparency of targeted advertising by clearly informing consumers about the nature of the advertisements they are receiving.

2. Requiring firms that engage in targeted advertising to ensure that consumers opt into such advertising.

3. Limiting the ability of advertisers to obtain the data required for targeted advertising through a range of data protection measures including: data protection-friendly default requirements (e.g., requiring granular but clear consent for data sharing, etc.).

4. Restricting or prohibiting the ability for firms to leverage dark patterns to obtain personal information used for targeting (e.g., default settings, hidden / complex information, sludge, or other patterns that manipulate consumers or obstruct them from understanding the implications of data sharing).

The Regulatory Review section provides a summary of the legislative and regulatory approaches being employed in Canada, the US, and the EU. Overall, current rules focus primarily on point 3 above, aiming to ensure that consumers have awareness and understanding when consenting to data sharing policies. However, newer rules are increasingly focused on identifying, labeling, and prohibiting the use of dark patterns and other similar deceptive design techniques.

Targeted advertising and retail investing

Although public data is limited, we know that targeted advertising is also used by popular, newer retail investing platforms. They will include their use of behavioural advertising practices in their terms of use, acknowledging that ad exchanges and data companies may use cookies and track data to deliver tailored ads.[111] We see similar practices from bank-owned, self-directed investing platforms. In their privacy code, the notes using "affiliates or other companies to provide services on our behalf, such as data processing, account administration, analytics, and marketing. Such companies will be given only the Personal Information needed to perform those services [...]."[112]

Forbes notes that because the target audience for many retail investing platforms (especially those that are "mobile-first") tend to be younger, "digitally native," and highly active across social media platforms, they are particularly strong candidates for targeted advertising.[113]

Some platforms have even faced public scrutiny for the use of their aggressive marketing techniques - in 2020, Massachusetts securities regulators filed a complaint against Robinhood for using aggressive advertising tactics that targeted younger individuals with

---

[111] Anonymized.

[112] Anonymized.

[113] Arora, K. (2022). The Rise of the Retail Investor. Forbes.

little, if any investment experience.[114]

Our literature scan did not reveal any research that addresses the impact of targeting retail investors in particular. Given the effectiveness of targeted advertising writ large, we believe that it is likely to be more effective than traditional mass advertising in customer acquisition - bringing on new users. All of the concerns described above related to privacy and data acquisition are relevant to investing platforms. Given the enormous potential impact of investment choices on a person's finances, there are particular concerns around potential targeting of vulnerable consumers (investors). However, we are unaware of any data or research on whether or how vulnerable people are being targeted and, if so, what the impact may be.

---

[114] Commonwealth of Massachusetts Office of the Secretary of the Commonwealth Securities Division. (2020). Administrative Complaint - Docket No. E-2020-0047.

Review of Regulatory Approaches

This section summarizes the current state of regulations that protect against the use of dark patterns, dark nudges, and targeted advertising on online interfaces. We examine the current regulatory environment in three jurisdictions - Canada, the United States (US), and the European Union (EU).

Table: Overview of Regulatory Approaches

Jurisdiction	Summary of Regulatory Environment
Canada	- Consumer protection authority, including protection against the techniques described in this report, is diffused across different statutes, policies, and codes of conduct, and enforced by different organizations at the federal, provincial, territorial, and municipal levels. - Regulatory bodies tend to use existing rules and mechanisms for enforcement action, rather than developing or updating statute or regulation. Enforcement action is concentrated on the protection of personal information (e.g., via insufficient user consent), with less attention to deceptive online choice architecture practices that do not relate to privacy. - In contrast to the overall trend we observed, the Competition Bureau of Canada has started updating legislation to call out dark patterns (e.g., drip pricing) and has taken relevant enforcement action against firms.
United States	- Regulatory bodies are using existing rules that limit unfair or deceptive practices (e.g., Federal Trade Commission Act) to take enforcement action against dark patterns. - Efforts are underway to amend or clarify existing rules to directly name dark patterns as a whole or specific types of dark patterns. - New legislation or regulation to address gaps in existing rules is under development. There has been a particular focus on data collection and privacy, but action extends to other uses of dark patterns, dark nudges, and sludge. - There is growing interest from the U.S. Securities and Exchange Commission and other investor protection organizations to explore and understand digital engagement practices used on investment trading platforms.
European Union	- The EU has seen a significant increase in regulatory guidance, discussion, and enforcement against the use of dark patterns and targeted advertising under the EU General Data Protection Regulation (GDPR) regime. - There are efforts underway to develop new regulatory

<table>
<tr>
<td></td>
<td>

frameworks, such as the Digital Services Act, to prohibit the use of dark patterns on online platforms. These will complement existing rules such as the GDPR and the Unfair Commercial Practices Directive and aim to close regulatory gaps that platforms can use to manipulate users.

● Regulatory bodies are focused on protecting the data and privacy of consumers and enforcing consent when data is collected (thus limiting the ability to collect data that could be used for targeted advertising).

</td>
</tr>
</table>

Canada

In Canada, the regulatory framework protecting consumers against dark patterns, dark nudges, and targeted advertising is relatively sparse. However, existing legislation includes stipulations that may be used to regulate dark patterns and targeted advertising.

● Personal Information Protection and Electronics Document Act (PIPEDA): PIPEDA applies to private sector organizations that collect, use, or disclose personal information in the course of a commercial activity. Under Principle 4.3.5, it requires organizations to obtain informed consent before collecting and using personal data, and prohibits obtaining consent through deception.[115] These rules restrict the collection of data that may otherwise enable forms of targeted advertising. Dark patterns that manipulate users into sharing personal information or engage in targeted advertising may be in violation of PIPEDA.[116][117]

The Office of the Privacy Commissioner of Canada is an independent agency that oversees the enforcement of PIPEDA. In recent years, it has released guidelines on privacy in online behavioural (targeted) advertising to ensure that practices are fair, transparent and in compliance with PIPEDA.[118] These include the importance of obtaining "meaningful consent" from users when collecting, using, and disclosing their personal information, and ensuring that consent processes are "understandable, user-friendly and customized to the nature of the product or service."[119]

● Canadian Anti-Spam Legislation (CASL): The CASL was created to protect consumers from unwanted electronic messages (such as spam).[120] Administered by the Canadian Radio-television and Telecommunications Commission, it requires organizations to obtain consent before sending commercial electronic messages.[121] In 2014, the CASL amended the Competition Act (see below) to prohibit "false and

---

[115] Morgan, C.S., Langlois, F., Gao, K., Lan, J. (2022). A Canadian Perspective on Regulating Dark Patterns.

[116] Government of Canada. (2000). Personal Information Protection and Electronic Documents Act (PIPEDA). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

[117] Office of the Privacy Commissioner of Canada. (2021). PIPEDA and Your Privacy Rights.

[118] Office of the Privacy Commissioner of Canada. (2011). Guidelines on privacy and online behavioural advertising - updated in 2021.

[119] Morgan, C.S., Langlois, F., Gao, K., Lan, J. (2022). A Canadian Perspective on Regulating Dark Patterns.

[120] Canadian Radio-television and Telecommunications Commission. (2022). From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent.

[121] Canadian Radio-television and Telecommunications Commission. (n.d.). Canada's Anti-Spam Legislation (CASL).

misleading statements in electronic messages that promote a business interest or a product."[122]

This law can be used to help regulate targeted advertising and deceptive practices that may be used in online marketing. Companies are required to obtain consent before sending electronic messages, and prohibited from using deceptive practices, including making false or misleading representations, or filing to disclose important information.

- Competition Act: Administered by the Competition Bureau, the Competition Act governs competition law in Canada and aims to prevent anti-competitive practices in the marketplace. It prohibits the use of false or misleading representations that may harm consumers.[123] This prohibition can and has been understood to include dark patterns. The Competition Bureau has publicly identified a number of practices that would be enforced under the Competition Act including: 74.01(1.1), deceptive use of testimonials (social norms) (section 74.02), bait and switch (section 74.04), and the use of promotional contests or deceptive prize notices. Following an amendment in 2022, the Act also prohibits drip pricing.

  Since 2015, the Competition Bureau has filed cases for the use of false or misleading representations on 37 instances. Notably, the Bureau penalized two large ticket exchange / sellers for misleading pricing claims in the online sale of tickets - it found that consumers could not buy tickets at advertised prices because they were charged additional mandatory fees during the later stages of the purchasing process - an example of drip pricing.[124]

- Digital Charter Implementation Act (Bill C-27): In 2022, the Canadian government proposed the Digital Charter Implementation Act, in order to modernize the framework for the protection of personal information in the private sector and introduce new rules for the development and deployment of artificial intelligence (AI).[125] This legislation aims to protect the privacy of Canadians by (1) increasing control and transparency when sharing personal information; (2) giving Canadians freedom to move their information in a secure manner, and (3) ensuring that information is destroyed when consent is withdrawn. The law contains provisions that could help regulate targeted advertising, such as meaningful consent, and prohibit deceptive practices that may be used in online marketing.

  Under the DCIA, companies would be required to obtain "meaningful consent"
  As part of this new regulatory framework, the Consumer Privacy Protection Act will be introduced to regulate deceptive privacy practices that undermine individuals' right to consent. This may further strengthen the Canadian government's enforcement power against dark patterns that undermine consumer privacy and mitigate the use of targeted advertising.

---

[122] Morgan, C.S., Langlois, F., Gao, K., Lan, J. (2022). A Canadian Perspective on Regulating Dark Patterns.

[123] Competition Bureau. (2020). Deceptive Marketing Practices Digest.

[124] Government of Canada. (2022). Deceptive marketing practices - Cases and outcomes.

[125] Government of Canada. (2022). Canada's Digital Charter: Trust in a digital world.

<u>Provincial Regulation:</u> The provinces of Alberta, British Columbia, and Quebec have private-sector privacy laws that are substantially similar to PIPEDA. Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have also adopted substantially similar legislation regarding the collection, use and disclosure of personal health information.

In addition, there is growing interest from the Ontario Securities Commission to explore and understand digital engagement practices used on investment trading platforms. In 2022, the OSC and BIT published "Digital Engagement Practices in Retail Investing: Gamification and Other Behavioural Techniques," a study that examined the influence of gamification and other behavioural techniques on retail investor behaviour.

In general, Canada sees consumer protections diffused across different statutes, regulatory policies, and mandatory / voluntary codes of conduct.[126] The effectiveness of these mechanisms may depend on enforcement frameworks that delineate clear lines of responsibility when multiple actors are involved. Current consumer protections are owned by different organizations at the federal, provincial, territorial, and municipal levels, through different regulatory mechanisms (e.g., statutes, policies, codes of conduct).[127] A clear understanding of how legal frameworks (such as PIPEDA) can be applied to this context, and who is responsible for enforcing them, and the adequacy of the enforcement remedies, is required.

United States

In recent years, there has been a prominent uptick in US regulatory research, rule-making, and enforcement action related to dark patterns, dark nudges, sludge, and targeted advertising. Key trends we see include:

1. Regulatory bodies using existing rules that limit unfair or deceptive practices (e.g., Federal Trade Commission Act) to take enforcement action against dark patterns;

2. The amendment or clarification of existing rules to directly name dark patterns as a whole or specific types of dark patterns;

3. The contemplation or development of new legislation or regulation to address gaps in existing rules. There has been a particular focus on data collection and privacy, but action extends beyond this;[128] and,

4. Growing interest from the U.S. Securities and Exchange Commission and other investor protection organizations to explore and understand digital engagement practices used on investment trading platforms.

While the majority of regulatory policies and enforcement actions below do not directly relate to securities, they paint a picture of how other consumer financial protection domains are

---

[126] Officer of the Privacy Commissioner of Canada. (2018). Summary of privacy laws in Canada.

[127] Government of Canada. (2018). Consumer protection legislation in Canada

[128] Congressional Research Service. (2022). What Hides in the Shadows: Deceptive Design of Dark Patterns. *CRS Reports - IF12246 Version 2.*

approaching this issue. There is an opportunity for securities regulators to build on this effort and develop similar protective measures for individual investors.

Federal Trade Commission: The Federal Trade Commission (FTC) is an independent agency of the United States government with a mandate of promoting consumer protection and stopping deceptive or unfair business practices in the marketplace, including those that take the form of dark patterns. It began releasing public guidance on the use of digital dark patterns in 2021.[129] As described further below, Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce" has been its most important tool in taking enforcement action against dark patterns, dark nudges, and sludge.

- In April 2021, the FTC hosted a public workshop to explore how user interfaces can have the effect of obscuring, subverting, or impairing consumer autonomy and decision-making. Officials discussed the rise of dark patterns in the digital marketplace, classified common dark patterns, and shared recommendations for companies.[130]

- In October 2021, the FTC followed up with an enforcement policy statement, committing to bring action against companies employing dark patterns that "trick and trap" consumers into subscription services. Although the statement only focused on one specific domain (subscription services), the use of dark patterns was defined as an unfair and deceptive practice under the Federal Trade Commission Act (FTC Act) and other laws.[131] Companies are now required to (1) disclose clearly and conspicuously all material terms of a product or service, (2) obtain the consumer's express informed consent before charging them for a product or service, and (3) provide easy and simple cancellation to the consumer.

- In September 2022, the FTC published the Bringing Dark Patterns to Light report, building on previous research efforts to identify and classify common dark patterns, and the manner in which they raise consumer protection concerns. This report also discusses many of the FTC's enforcement actions against companies that have violated Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[132]

- In March 2023, the FTC formally proposed a "click to cancel" rule that requires sellers to "make it as easy for consumers to cancel their enrollment as it was to sign up."[133] This is part of the FTC's ongoing review of its 1973 Negative Option Rule, used to combat unfair or deceptive practices related to subscriptions, memberships, and other recurring-payment programs. The amended rule would apply to all subscription features in all media and aim to: (a) set clear, enforceable, performance-based

---

[129] Federal Trade Commission. (2022). About the FTC.

[130] Federal Trade Commission. (2022). Bringing Dark Patterns to Light.

[131] Morgan, C.S., Langlois, F., Gao, K., Lan, J. (2022). A Canadian Perspective on Regulating Dark Patterns.

[132] Federal Trade Commission. (2021). FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions - Enforcement Policy Statement.

[133] Federal Trade Commission. (2023). Federal Trade Commission Proposes Rule Provision Making it Easier for Consumers to "Click to Cancel" Recurring Subscriptions and Memberships

requirements; (b) make sure people understand and agree to what they're buying; and (c) make sure people can cancel without jumping through lots of hoops.[134]

There is debate regarding the comprehensiveness of the FTC Act. While some believe that Section 5 of the FTC Act is sufficient to regulate harmful dark patterns, others have called on the FTC to expand its mandate and include the use of "manipulative" or "abusive" practices.[135]

The FTC has in place other regulations that some dark patterns may violate. The table below provides additional details:

Regulation or Act	Summary
Restore Online Shoppers' Confidence Act (ROSCA)	Prohibits any post-transaction third party seller (a seller who markets goods or services online through an initial merchant after a consumer has initiated a transaction with that merchant) from charging a consumer in an Internet transaction unless it has disclosed clearly all material terms of the transaction and obtained the consumer's express informed consent to the charge.[136] It is intended to protect consumers from deceptive online marketing practices and requires online sellers to provide clear disclosures regarding terms of their transactions.
Truth in Lending Act (TILA)	Requires lenders to provide consumers with loan cost information so that they can comparison shop for certain types of loans. This may protect consumers from dark patterns such as hidden or complex information.[137]
Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM)	Establishes requirements for those who send unsolicited commercial email. It bans false or misleading header information, prohibits deceptive subject lines, requires that unsolicited commercial email be identified as advertising, and provides recipients a method for opting out. The Act directs the FTC to issue rules requiring the labeling of sexually explicit commercial email and establishing the criteria for determining the primary purpose of a commercial email.[138] While CAN-SPAM does not directly regulate targeted advertising, it provides a framework for how companies can use email-based advertising in compliance with federal law.
Children's Online Privacy Protection Act (COPPA)	Imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal

---

[134] Federal Trade Commission. (2023). Fact Sheet: Proposed Changes to the FTC's Negative Option Rule.

[135] Congressional Research Service. (2022). What Hides in the Shadows: Deceptive Design of Dark Patterns. *CRS Reports - IF12246 Version 2.*

[136] Federal Trade Commission. (2010). Restore Online Shoppers' Confidence Act: Law 15 U.S.C. §§ 8401-8405.

[137] Consumer Financial Protection Bureau. (2015). Truth in Lending Act.

[138] Federal Trade Commission. (2003). Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM): 15 U.S.C §§ 7701-7713.

	information online from a child under 13 years of age.[139] This may protect the privacy of children and limit their exposure to dark patterns and targeted advertising.
Equal Credit Opportunity Act (ECOA)	Prohibits creditors from discriminating against credit applicants on the basis of race, color, religion, national origin, sex, marital status, age, because an applicant receives income from a public assistance program, or because an applicant has in good faith exercised any right under the Consumer Credit Protection Act.[140] This may protect consumers from discriminatory and targeted practices.

Additional federal legislation that would constrain the use of dark patterns is currently pending in the Senate (Deceptive Experiences to Online Users Reduction Act (DETOUR Act), Senate Bill 1084, 116th Congress, introduced April 9, 2019).[141]

In 2022, the FTC ordered a large video game and software developer to pay $520 million over violations of the Children's Online Privacy Protection Act (COPPA). The FTC found that the developer deployed dark patterns - specifically privacy-invasive default settings and deceptive interfaces - to trick users, including teenagers and children, and manipulated users into making unintentional purchases. It also collected personal information from children without notifying parents or obtaining their parents' verifiable consent. This is the FTC's largest administrative order in history.[142]

The FTC also uses its authority to protect users against harmful advertising practices. Since the mid-1990s, the FTC has provided guidance on the regulation of online behavioural advertising.[143] It has also proposed legislative frameworks and bills to regulate this practice.[144][145] These have not yet been formally passed.

The FTC has also used existing legislation (the FTC Act) to enforce actions against organizations engaged in harmful targeted advertising:

- In 2022, it charged a large social media platform with deceptively using account security data to sell targeted ads. Users were asked to share contact information (phone numbers and email addresses) to protect their accounts - the company then profited by allowing advertisers to use this data to target specific users. The company was ordered to pay a $150 million penalty and was banned from profiting from its deceptively collected data.[146]

---

[139] Federal Trade Commission. (1998). Children's Online Privacy Protection Rule ("COPPA"): 16 CFR Part 312.

[140] The United States Department of Justice. (2022). The Equal Credit Opportunity Act.

[141] Luguri, J. and Strahilevitz, L.J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis 2021: Volume 13.*

[142] Federal Trade Commission. (2022). Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges.

[143] Federal Trade Commission. (2009). Staff Report on Self-Regulatory Principles for Online Behavioral Advertising.

[144] United States Congress. (2011). Summary: H.R.654 — 112th Congress (2011-2012)

[145] United States Congress. (2011). Summary: S.799 — 112th Congress (2011-2012)

[146] Federal Trade Commission. (2022). FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads.

- In 2023, the FTC issued a proposed order banning an online counseling service from sharing consumers' health data, including sensitive information about mental health challenges, for advertising. This company was also ordered to pay $7.8 million to consumers after it revealed sensitive data with third parties, including large social media platforms. It was found to be in violation of the Health Insurance Portability and Accountability Act (HIPAA) and the FTC Act.[147]

Consumer Financial Protection Bureau: The Consumer Financial Protection Bureau (CFPB), established under the Consumer Financial Protection Act (CFPA) of 2010, was created to serve as the U.S. government's primary regulator of consumer financial products.[148] Its mission is to ensure markets for consumer financial products are fair, transparent, and competitive. Like the FTC, the CFPB has also enforced action against companies that use unfair, deceptive, or abusive practices related to consumer financial products and services. In 2022, the CFPB took action against a consumer credit reporting company for employing multiple digital dark patterns in order to profit from consumers (specifically, to trick customers into recurring payments that are difficult to cancel). The CFPB alleged that the company violated the Consumer Financial Protection Act of 2010 by engaging in deceptive acts and practices. This is a longstanding Act that can be used for enforcement against dark patterns.

U.S. Securities and Exchange Commission: The U.S. Securities and Exchange Commission (SEC), established in 1929, is an independent agency of the United States government that protects investors, maintains fair, orderly, and efficient markets, and facilitates capital formation.[149]

The SEC has begun investigating the use of dark patterns in the space of online investment trading. In 2021, it requested public comment on matters related to the use of digital engagement practices by broker-dealers and investment advisers. These practices include behavioural prompts, differential marketing, game-like features (i.e., gamification), and other design elements or features designed to engage with retail investors on digital platforms.[150] The SEC acknowledged that such features could encourage investors to trade more often, invest in different products, or change their investment strategy. It was interested in understanding if investors are appropriately protected.[151]

Since this request, there are growing calls for the SEC to take action against dark patterns. Large investor protection organizations, such as the North American Securities Administrators Association (NASAA) have called for the use of "dark patterns" in investment applications and platforms to be prohibited. NASAA has stated that "investors derive no benefit from features that frustrate their intentions, whether that be closing" an account, removing services, or making trades."[152]

---

[147] Federal Trade Commission. (2023). FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising.
[148] ibid.
[149] U.S. Securities and Exchange Commission. (2022). What We Do.
[150] U.S. Securities and Exchange Commission. (2021). Request for Information and Comments on Broker-Dealer and Investment Adviser Digital Engagement Practices, Related Tools and Methods, and Regulatory Considerations and Potential Approaches; Information and Comments on Investment Adviser Use of Technology to Develop and Provide Investment Advice.
[151] ibid.
[152] North American Securities Administrators Association. (2021). Response to File No. S7-10-21: Request for Information and Comments on Broker-Dealer and Investment Adviser Digital Engagement Practices, Related Tools and Methods, and

<u>State Regulation:</u> Individual states have enacted legislation to regulate specific types of dark patterns. In March 2021, California became the first to define dark patterns and pass consumer privacy legislation banning the use of them. The California Privacy Rights Act (CPRA), which will be enforced in 2023, expands the California Consumer Privacy Act (CCPA) and defines dark patterns as a "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation."[153] It forbids the use of dark patterns to obtain consent related to the processing of personal information, which can protect users against targeted advertising.[154]

The states of Colorado and Connecticut have followed suit, regulating dark patterns under the Colorado Privacy Act and the Connecticut Data Privacy Act.[155] Other states, such as Washington, are also in the process of developing similar legislation.

European Union

In the European Union (EU), the issue of dark patterns (including dark nudges and sludge) and targeted advertising have gained the attention of regulatory and policy bodies. Key trends include:

1. An increase in regulatory guidance, discussion, and enforcement against the use of dark patterns and targeted advertising under the EU General Data Protection Regulation (GDPR) regime.

2. Efforts to develop new regulatory frameworks, such as the Digital Services Act, to prohibit the use of dark patterns on online platforms. These will complement existing rules such as the GDPR and the Unfair Commercial Practices Directive and aim to close regulatory gaps that platforms can use to manipulate users.[156]

3. A focus on protecting the data and privacy of consumers and enforcing consent when data is collected (thus limiting the ability to collect data that could be used for targeted advertising).

<u>General Data Protection Regulation:</u> Protective measures in the EU relate primarily to the use of dark patterns, targeted advertising, and their effect on privacy and consent. Through its General Data Protection Regulation (GDPR), the EU has built a regulatory and legal framework signaling its commitment to protecting consumers' data and privacy. The GDPR consists of a set of regulations that EU member states must adhere to in order to protect digital data and privacy. These are likely to significantly curtail the ability of firms, including investment firms, to engage in targeted advertising. Key provisions of the GDPR include:

- A requirement that companies must obtain **clear, informed, and active consent** from users when asking them to opt into privacy policies. Articles 7 and Recitals 32,

---

Regulatory Considerations and Potential Approaches; Information and Comments on Investment Adviser Use of Technology to Develop and Provide Investment Advice.

[153] National Law Review. (2021). Dark Patterns Come to Light in California Data Privacy Laws.

[154] Morgan, C.S., Langlois, F., Gao, K., Lan, J. (2022). A Canadian Perspective on Regulating Dark Patterns.

[155] Stauss, D., and Weber, S. (2022). How do the CPRA, CPA & VCDPA treat dark patterns?

[156] European Commission. (2023). Consumer protection: manipulative online practices found on 148 out of 399 online shops screened.

42, and 43 of the Regulation require that companies procure consent lawfully, "by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her."[157]

The European Data Protection Board (EDPB): Mandated to ensure consistent application of the GDPR - notes in their Guidelines on Consent that "consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them." Consent cannot be freely given when "access to services and functionalities [is] made conditional on the consent," or when the data subject is "unable to refuse or withdraw his or her consent without detriment," or when "the process for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively." Without this consent, the data collection activity is rendered unlawful.[158]

- Requirements enforcing companies to **build data protection and privacy into their design, and provide privacy by default**. Recital 78 states that, "when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications… " Data protection or privacy by default requires that consumers should receive a high level of data protection, even if they do not opt out of the collection and processing of personal data.[159] In their guidelines to support this Article, the EDPB notes that "data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design".[160]

- Requirements enforcing the principle of **purpose limitation**. Article 25 requires data controllers to ensure that they process "… only personal data which are necessary for each specific purpose of the processing. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility."[161] Data controllers should also collect the minimum amount required to perform a task, and explain to consumers, in a clear manner, what personal data is collected, and for what purposes.

In March 2022, the EDPB shared "Guidelines on dark patterns in social media platform interfaces: how to recognize and avoid them", intended to "offer practical recommendations to designers and users of social media platforms on how to assess and avoid so-called "dark

---

[157] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[158] European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.

[159] European Data Protection Supervisor. (2018). Opinion 5/2018: Preliminary Opinion on privacy by design.

[160] Adeyoju, A. (2022). Privacy Dark Patterns: A Case for Regulatory Reform in Canada.

[161] Forbrukerradet (Norwegian Consumer Council). (2018). Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy.

patterns" in social media interfaces that infringe on GDPR requirements".[162] In these guidelines, the EDPB defines (privacy) dark patterns as "interfaces and user experiences implemented on social media platforms that cause users to make unintended, unwilling and potentially harmful decisions regarding the processing of their personal data." These new Guidelines demonstrate an ongoing commitment to the regulation of privacy dark patterns in the EU.

Building on the GDPR, the EU has also developed the Digital Services Act (DSA) (enforced in November 2022) to regulate online marketplaces and the "obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content."[163] The DSA is intended to act as a transparency and accountability framework for online platforms. One stipulation is a ban on the use of dark patterns on the interface of online platforms, including tricks to "deceive, manipulate, or otherwise materially distort" a user's ability to make free and informed decisions.[164] Another requires "wide ranging transparency measures for online platforms, including better information on terms and conditions… and algorithms for recommending content or products to users."[165]

European Securities and Markets Authority: The European Securities and Markets Authority (ESMA) is the EU's financial markets regulator and supervisor. It aims to enhance investor protection, promote orderly financial markets, and safeguard financial stability.

In recent years, ESMA has worked under the Markets in Financial Instruments Directive (MiFID II) legislation to tighten investor protection measures. In 2022, it put forward proposals to the European Commission, in response to a request for advice on retail investor protection. Recommendations related to the use of dark patterns and targeted advertising included:[166]

- Addressing **information overload** by proposing to define what is vital information and by using digital techniques such as layering of information;
- Developing a **standard EU format of information on costs and charges** and aligning the disclosures under MiFID II and other relevant regulations;
- Addressing issues related to misleading marketing campaigns on social media and the use of online engagement practices, such as the **use of gamification techniques** by firms or third parties;
- Addressing **aggressive marketing communications**; and
- Giving authority to National Competent Authorities (NCAs) and ESMA to impose on firms the use of risk warnings for specific financial instruments.[167]

These recommendations remain with the Commission for further investigation, comment, and/or adoption.

---

[162] European Data Protection Board. (2022).Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them.

[163] European Commission. (2022). Questions and Answers: Digital Services Act.

[164] ibid.

[165] ibid.

[166] European Commission. (2022). ESMA makes recommendations to improve investor protection.

[167] ibid.

Building on ESMA's efforts, EU member states have also taken individual action against the use of dark patterns in retail investing. In 2022, the German Federal Financial Supervisory Authority (BaFin) issued guidance around the use of dark patterns on trading apps.[168] BaFin has drawn attention to a number of specific dark patterns, including sensory manipulations (e.g., "having no or a barely perceptible button to cancel a transaction" while "having a strikingly designed button to conclude a transaction"), as well as the use of cookie banners that require users to click multiple buttons to avoid accepting cookies. BaFin has based this guidance on Section 63 (6) of the German Securities Trading Act (WpHG), which is part of the code of conduct for investment firms, and implements Article 24 (3) of the MiFID II into national law.[169]

---

[168] Bundesanstalt für Finanzdienstleistungsaufsicht. (2022). BaFin: Dark Patterns in Trading Apps unzulässig.

[169] Beck, B., Leach, C., Scholl, P., and Worm, U. (2022). German Authority and EU Bodies Target "Dark Patterns" in Trading Apps and Online Interfaces.

Recommendations and considerations for regulators and other stakeholders

In a fiercely competitive online landscape, investing platforms for self-directed retail investors are using behavioural science to design new digital engagement and marketing practices that influence investor decision making. Some of these approaches have generated regulatory concerns due to their potential impact on investors' financial wellbeing and privacy protections. Following the OSC's previous report on the gamification of investing platforms,[170] this report examined a subset of techniques labelled as dark patterns, dark nudges, sludge, and targeted advertising.

From our research, we learned that the existing evidence base has enormous gaps, a result of the rapid pace of change in the industry and the relatively sparse data that platforms have shared with researchers and the public. Despite these challenges, this report presents a coherent set of definitions and a detailed, wide-ranging taxonomy of key techniques that fit under the categories of dark patterns, dark nudges, sludge, and targeted advertising.

We also found that these four techniques are prevalent and have the potential to negatively impact investor welfare. Areas of particular concern include techniques used to disguise the cost of investing (e.g., hidden fees and information), to obtain personal information without informed consent (e.g., complex terms and services, defaults), and to make it harder to withdraw funds, close an account, or stop a premium subscription service (e.g., sludge and process frictions).

We believe the technique classification developed in this report is a critical input to more informed regulatory discussion and action, and represents a leading resource not just in Canada - but internationally. Around the world, we see increased efforts to better understand harmful online practices from a lens of consumer protection. Regulatory bodies in the United States and the European Union are amending current regulatory frameworks and enacting new legislation and regulation to control unfair and deceptive practices. In particular, enforcement action is concentrated on data protection and privacy (thus limiting the ability to collect data that could be used for targeted advertising), but activities extend to other uses of dark patterns, dark nudges, and sludge. This includes recent efforts by the Federal Trade Commission (FTC) to identify and classify common dark patterns, pursue enforcement actions when companies have violated the FTC Act even where the dark patterns are not specifically noted in the Act, and propose new rules in response to unfair practices (e.g., a "click to cancel" rule that makes it easy for consumers to cancel memberships and subscriptions). Similarly, the German Federal Financial Supervisory Authority (BaFin) has issued guidance around the use of dark patterns on trading apps, drawing attention to dark patterns and targeted advertising techniques. Regulatory bodies in Canada have started taking similar actions. For example, the Competition Bureau of Canada has publicly identified a number of deceptive practices that would be enforced under the Competition Act. Following an amendment in 2022, the Act now specifically prohibits drip pricing. Overall, there appears

---

[170] Ontario Securities Commission. (2022). Digital Engagement Practices in Retail Investing: Gamification & other Behavioural Techniques.

to be opportunity for further regulatory and enforcement responses in Canada based on comparison to the EU and US.

Our research revealed potential risks created by dark patterns, dark nudges, sludge, and targeted advertising:

- Requiring users to **opt-in to certain features that can constitute dark patterns or dark nudges,** including most prompts (e.g., price movement notifications) and ranked lists (e.g., platform-specific top-traded lists).

- **Targeted advertising based on data that was not obtained through informed consent**.

- **Targeted advertising by investing platforms to vulnerable customers, including people with cognitive limitations and users likely to be new to or unfamiliar with online environments**.

- **Complex language** within fee schedules, privacy protections, and restrictions on withdrawing funds.

- **The removal of process steps in trade execution**.

- The **difficulty for customers to cancel subscriptions, close accounts, and withdraw funds.**

Appendix A: Dark Patterns, Dark Nudges, & Sludge on Investing Platforms

The following table summarizes the findings of our environmental scan, noting which dark patterns, dark nudges, and sludge were observed on each. This was an exercise that required significant judgment because not every use of the technique is a dark pattern, nudge, or instance of sludge. For example, reminders to finish account creation will generally be aligned to user interests and preferences, and therefore are not a dark pattern. Our observation of each platform was limited to the core user journey (account creation, deposit, trading, and withdrawal). We were not able to test all features of all platforms (e.g., those that required larger balances). The scan took place from Nov 2022 - Jan 2023.

	Location	Device / Type of Review	Use of Dark Patterns, Dark Nudges, and Sludge on Investing Platforms										
			Dark Patterns							Dark Nudges		Sludge	
			Prompts & Reminders	Intermediate Currency	Ranking	Sensory Manipulations	Social Norms & Interactions	Scarcity Claims	Hidden fees (drip pricing)	Removal of Process	Defaults	Process Friction	Complex language
A	Canada	iOS	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes
B (registered)	Canada	iOS	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
C	Canada	iOS / Web search[171]	No	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes
D	Canada	iOS	No	No	No	No	No	Yes	Yes	No	Yes	Yes	Yes
E	Canada	Desktop	No	Yes	No	No	No	No	No	Yes	Yes	No	Yes
F	US	Web search	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes

---

[171] Note: In some instances, we were not able to conduct audits of a platform given logistical barriers (e.g., jurisdictional restrictions or high minimum trading requirements). In these cases, we conducted a web search, or a review of publicly available information about the interface and features of a platform. This included resources provided by the platform, video "walkthroughs" or demonstrations, and user reviews of their experiences on these platforms.

G (unregistered)	UK	iOS / Web search	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
H (registered)	Canada	iOS	Yes	No	Yes	No	No	No	Yes	Yes	Yes	No	Yes
I (unregistered)	Canada	iOS	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes
J (registered)	Canada	iOS	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes

Appendix B: Works Cited

Adeyoju, A. (2022). Privacy Dark Patterns: A Case for Regulatory Reform in Canada.

Andraszewicz, S., Kaszás, D., Zeisberger, S., & Hölscher, C. (2022). The influence of upward social comparison on retail trading behavior.

Alter, A. L., & Oppenheimer, D. M. (2008). Easy on the mind, easy on the wallet: The roles of familiarity and processing fluency in valuation judgments. *Psychonomic bulletin & review*, *15*(5), 985-990.

Arnold, M., Pelster, M., & Subrahmanyam, M. G. (2022). Attention triggers and investors' risk-taking. *Journal of Financial Economics*, *143*(2), 846-875.

Barber, B. M., Huang, X., Odean, T., & Schwarz, C. (2022). Attention-induced trading and returns: Evidence from Robinhood users. *The Journal of Finance*, *77*(6), 3141-3190.

Behavioural Insights Team. (2019). Best Practice Guide - Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses.

Birner, K. (2015). One click to empowerment?: Opportunities and challenges for labour in the global value chain of e-commerce. International Journal of Labour Research, 7(1/2), 55.

Chaudhry, S., & Kulkarni, C. (2021, June). Design Patterns of Investing Apps and Their Effects on Investing Behaviors. In *Designing Interactive Systems Conference 2021* (pp. 777-788).

Dinner, I., Johnson, E. J., Goldstein, D. G. and Liu, K. (2011). Partitioning Default Effects: Why People Choose not to Choose. *Journal of Experimental Psychology: Applied*, 17(4): 332–341.

European Data Protection Supervisor. (2022). Privacy by Default.

EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

Federal Trade Commission. (2022). Bringing Dark Patterns to Light.

Federal Trade Commission. (2020). FTC Complaint: FTC v. Age of Learning, Inc., also d/b/a ABCmouse and ABCmouse.com, Case No. 2:20-cv07996.

Gawronski, B., and Creighton, L. A. (2013). Dual process theories. Oxford University Press.

Ghose, A., Goldfarb, A., and Han, S. P. (2013). How Is the Mobile Internet Different? Search Costs and Local Activities. Information Systems Research, 24(3), 613–631.

Glaze, J. (2022). Fast-Thinking Attention and the Disposition Effect. *Available at SSRN 4121793*.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI conference on human factors in computing systems (pp. 1-14).

Jachimowicz, J., Duncan, S., Weber, E., & Johnson, E. (2019). When and why defaults influence decisions: A meta-analysis of default effects. *Behavioural Public Policy, 3*(2), 159-186.

Johnson, E., Bellman, S., and Lohse, G.L. (2002). Defaults, Framing and Privacy: Why Opting In-Opting

Kahneman, D., & Tversky, A. (1977). Prospect Theory. An Analysis of Decision Making Under Risk. doi:10.21236/ada045771

Kalda, A., Loos, B., Previtero, A., & Hackethal, A. (2021). *Smart (Phone) Investing? A within Investor-time Analysis of New Technologies and Trading Behavior* (No. w28363). National Bureau of Economic Research.

Kelleher, D. M., Grimes, J., & Chovil, A. (2022). Securities—Democratizing Equity Markets with and Without Exploitation: Robinhood, Gamestop, Hedge Funds, Gamification, High Frequency Trading, and More. *Western New England Law Review*, *44*(1), 51.

Kelleher, Rowan. (2022). New York AG Slaps Online Travel Company with $2.6 Million Fine, Citing Predatory Behavior. Forbes.

King, D., and Delfabbro, P. (2018). Internet gaming disorder: Theory, assessment, treatment, and prevention. Academic Press.

Li, Y., Zhao, C., & Zhong, Z. K. (2021). Trading behavior of retail investors in derivatives markets: Evidence from Mini options. *Journal of Banking & Finance*, *133*, 106250.

Loewenstein, G. (2005). Hot-cold empathy gaps and medical decision making. Health Psychology, 24(4S), S49.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.

Moss, A. (2022). How Do Brokerages' Digital Engagement Practices Affect Retail Investor Information Processing and Trading?. Working Paper.

Nijboer, R. (2021). Retail investing in the information age: an investigation of herd behaviour on Robinhood. (Doctoral dissertation).

Obar, J., and Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, *Information, Communication & Society,* 23:1, 128-147.

Out1. *Marketing Letters* 13, 1 (01 Feb 2002), 5–15.

Raghubir, P., & Srivastava, J. (2008). Monopoly money: The effect of payment coupling and form on spending behavior. Journal of experimental psychology: Applied, 14(3), 213.

Rakovic, I. (2022). *Dark finance: Exploring deceptive design in investment apps* (Master's thesis, NTNU).

Reber, R., and Schwarz, N. (1999). Effects of Perceptual Fluency on Judgments of Truth. Consciousness and Cognition, 8(3), 338–342.

Richard A, Richard J, Johnston W, Miyasaki J. (2018). Readability of advance directive documentation in Canada: a cross-sectional study. *CMAJ Open*. 6(3):E406-E411.

Shah, A. K., and Oppenheimer, D. M. (2007). Easy does it: The role of fluency in cue weighting.

Soman, D., Cowen, D., Kannan, N., and Feng, B. (2019). Seeing sludge: Towards a dashboard to help organizations recognize impedance to end-user decisions and action (Research Report Series Behaviourally Informed Organizations Partnership). Research Report Series Behaviourally Informed Organizations Partnership.

Stein, R. (2020). The Top 5 Predictable Effects of New Entries in Robinhood's '100 Most Popular' List. *Available at SSRN 3694588*

Tan, G. K. S. (2021). Democratizing finance with Robinhood: Financial infrastructure, interface design and platform capitalism. *Environment and Planning A: Economy and Space*, *53*(8), 1862-1878.

The Committee of Advertising Practice. (2021). Guidance on advertising in-game purchases. https://www.asa.org.uk/static/4028c436-5861-4035- 8d98c148d3c66b7e/Guidance-on-advertising-in-game-purchases.pdf

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *science*, *185*(4157), 1124-1131.

UK, G. Research and analysis Evidence review of Online Choice Architecture and consumer and competition harm.

Ontario Securities Commission – Investor Office Research and Behavioural Insights Team (IORBIT)

Tyler Fleming
Director, Investor Office
tfleming@osc.gov.on.ca

Matthew Kan
Senior Advisor, Behavioural Insights
mkan@osc.gov.on.ca

Marian Passmore
Senior Advisor, Policy
mpassmore@osc.gov.on.ca

Patrick Di Fonzo
Senior Advisor, Behavioural Insights
pdifonzo@osc.gov.on.ca

Meera Paleja
Program Head, Investor Research
and Behavioural Insights
mpaleja@osc.gov.on.ca

Behavioural Insights Team (BIT)

Laura Callender
Senior Advisor
laura.callender@bi.team

Amna Raza
Senior Advisor
amna.raza@bi.team

Sasha Tregebov
Director, BIT Canada
sasha.tregebov@bi.team