Investigating the Data in Investor Alerting Portals

David M. Nichols[1*], Chris Chew[1] and Vimal Kumar[1]

[1]Department of Computer Science, University of Waikato, Hamilton, 3240, New Zealand.

*Corresponding author(s). E-mail(s): dmn@cs.waikato.ac.nz;
Contributing authors: cc246@students.waikato.ac.nz;
vimal.kumar@waikato.ac.nz;

Abstract

Financial regulators in many jurisdictions publish investor alerts that identify newly identified threats such as imposter websites and unlicensed firms. Many of these lists are aggregated by the *International Organization of Securities Commissions*. We analyse these alerts to understand if they can be used to create cybersecurity measures to protect consumers. An exploratory study indicates that the dangerous websites identified in the alerts are largely not detected by the safety services in web browsers. The financial security of consumers can be improved through coordination between the financial regulators, browser developers and cybersecurity services. We provide recommendations for improving the effectiveness of investor alerts through better data publication practices.

Keywords: Investor alerting, Cybersecurity, Financial crime, Financial regulators, Open data

1 Introduction

Financial scams are global problem (Kadoya et al. 2020). Netsafe, New Zealand reports that in 2023 New Zealanders potentially lost $2.3 billion to financial scams, representing 0.6% of the country's GDP (Abraham et al. 2024). The report further states that nearly 60% of New Zealanders deal with scams at least once per month while 50% have experienced a rise in scam encounters. These scams can take many forms including shopping scams, advance fee scams, fake invoice scams, romance scams, investment scams, Ponzi schemes, identity theft etc. In this paper, we specifically focus on investment scams, which in the Netsafe report was one of the top three scams experienced

Nichols, D.M., Chew, C. and Kumar, V. (2026) Investigating the data in investor alerting portals. *Security Journal*, 39(1) Article 9. https://doi.org/10.1057/s41284-025-00525-w

by New Zealanders. The Financial Markets Authority (FMA) of New Zealand claims that about one in five New Zealanders have been targeted by an investment scam (FMA 2024). These statistics highlight the need to examine the mechanisms intended to prevent such scams, and their effectiveness.

To counter the threat of investment scams, industry regulators around the world publish investor alerts describing newly identified threats within their jurisdictions. These warnings typically identify the entities involved and provide relevant background information (e.g., website URLs, emails, telephone numbers, postal addresses etc.). The web-based nature of many financial scams is reflected in the prevalence of URLs in the alerts. Most regulators publish a collection of such warnings. These datasets are valuable resources for protecting consumers against scams. Some financial institutions direct their customers to these portals for awareness while some regulators even use the number of warnings issued as a measure of success against scams. We aim to address the question: is the data in investor alerting portals useful for cybersecurity?

In this paper, we first provide an overview of investor alerting portals and then analyse how the alerts are published by a selection of financial regulators. Using URLs from recent alerts, we show that safety services in web browsers do not detect the reported websites as dangerous. We conclude with recommendations for more effective investor alerting, including improved dissemination, structuring and digital licensing.

2 Background

Jurisdictions around the world have empowered regulators to manage various aspects of their financial systems. Examples of financial regulators include the *Financial Conduct Authority (FCA)* in the UK and the *Financial Markets Authority (FMA)* in New Zealand. These regulators often provide an investor alerting service to inform both institutions and individuals of security threats to the financial system. These alerts include information on phishing websites, companies trading without necessary licenses, investment scams and other fraudulent practices. The *International Organization of Securities Commissions* (IOSCO) also provides a portal that aggregates investor alerts from its members. All these portals are published as websites.

IOSCO is an umbrella organization of financial regulators that "is officially committed to setting securities standards for global securities markets, infrastructures, investors, and intermediaries" (Marcacci 2023, 34). IOSCO has 131 ordinary members but these are institutions (e.g. Central Bank of Bahrain) and do not directly map to countries. Several organisations in Canadian provinces are members (e.g. *Alberta Securities Commission* and the *Autorité des marchés financiers* in Quebec) and the USA has two members (*Securities and Exchange Commission* and *Commodity Futures Trading Commission*). There are also non-voting members (e.g. *Ministry of Finance of the Republic of Belarus*, *Reserve Bank of Fiji*) alongside other organisations (e.g. *European Commission*, *Asian Development Bank*). All members appear to be able to contribute to the IOSCO Investor Alerts Portal. However, participation is voluntary and the portal "is not a complete list of all alerts and warnings from all IOSCO members" (IOSCO 2024b). For example, the 'Investor Alert List' published by the *Monetary Authority of Singapore* (MAS 2024) is not represented in the IOSCO portal.

The FMA in New Zealand derives its powers from various laws and regulations governing the financial markets. The FMA 'Warnings and alerts list' is one of many statutory tools used as part of its regulatory response against unlawful conduct (FMA 2016). The goal of providing the scam warnings on the investor alert list is to "inform and warn public/market about unlawful behaviour" and to minimise the impact of the scam (FMA 2016).

Most of these warnings can be categorised, with increasing specificity, as confidence frauds (Sood and Bhushan 2020), financial scams (Reurink 2018) and investment scams (Reurink 2018). Many of the alerts involve Authorised Push Payment (APP) scams (Braithwaite 2024; Doeland 2019): where the victim is tricked into trusting a person (or website) starting a sequence of interactions ending in a bank transfer to an account controlled by the attackers (Dahlgreen 2023). Although there is some commentary on warnings by regulators on general topics (e.g. initial coin offerings of cryptocurrencies (Dobrauz-Saldapenna and Klebeck 2019; Zetzsche et al. 2019)) we cannot find prior research on the content or effectiveness of investor alerting portals for more general financial scams.

Whilst these warnings can be accessed by the general public there seems to be little evidence on whether the public are actually aware of them. In the UK the FCA report that "27,544 people accessed the warning list" in 2022 (FCA 2023, 40), but there is no further exploration of whether the alerts are actually preventing any incidents. The alerts may be in a similar situation to broader efforts in investor education: that it is difficult to prove they actually reduce financial crime (Rutledge 2022).

Figure 1 shows a recent investor alert published by the FMA in New Zealand. This alert:

- labels the website of *NZX Wealth Investments* (nzxwealth.com) as an "imposter website"
- states that *NZX Wealth Investments* is not "associated with the New Zealand company, NZX Wealth Technologies Limited"
- reports that *NZX Wealth Investments* is "not registered on the Financial Service Providers Register"
- recommends caution and highlights returns which appear to be "unrealistically large"

Each of these four aspects of the alert are common cybersecurity topics: a phishing website, deceptive name similarity, a list of trusted entities and abnormal financial rewards. Alert titles cover a wide range of issues, including: "Deepfake video scam warning: fake news stories, political endorsements - multiple trading platforms", "Backchain Cibersecurity Department; Blockchain-dep.com; Au-blockchain.com; Crypto Fraud & Asset Recovery – Recovery scams" and "LBLV – Withholding funds, suspected scam".

Some alerting portals are explicitly suggested to consumers as a defensive measure. For example, the *Bank of New Zealand* recommends that their customers "check the FMA 'Warnings and alerts' page to make sure the firm isn't listed as a suspected scammer" (Bank of New Zealand 2024). Some alerts are presented as part of broader public financial education resources: the alerts on the Australian *Moneysmart* website

Fig. 1 An Investor Alert published on the website of the FMA in New Zealand (https://www.fma.govt.nz/library/warnings-and-alerts/nzx-wealth-investments/)

are placed alongside information on banking, insurance and retirement. The "investor alert list can help you know which companies, businesses and websites (or 'entities') are not to be trusted" (Moneysmart 2024). The *MoneySmart* and the *FCA* websites explicitly suggest and link to the global IOSCO alert list as a further source of information on investment scams.

In summary, regulators around the world publish investor alerts on their websites to inform consumers of a variety of financial threats. Financial institutions also direct their customers to the alerting portals as an additional defensive measure. However, we can find no prior work on understanding these alerts or whether they are indeed used by the public. There is a similar lack of analysis for the aggregated worldwide alerts published by IOSCO.

3 Analysis of the Investor Alerting Portals

Table 1 shows a selection of investor alerting portals: from IOSCO members and IOSCO's global aggregation. These publishers are part of government-mandated financial regulation in their jurisdictions. We restrict ourselves to reports and alerts from IOSCO members that are published in English. Analysing reports across the full diversity of global languages and jurisdictions is a large task beyond the scope of this paper.

Table 1 Overview of Selected Investor Alerting Portals (at 2024-03-26)

Publisher	Abbrev.	Area	Role	Alerts	Reporting Dates		Data	
					Earliest	Latest	Format	API
Financial Markets Authority	FMA	New Zealand	"conduct regulator of financial markets" (FMA 2023, 11)	577	2010-10-27	2024-03-21	CSV	—
Moneysmart (ASIC)	ASIC	Australia	"integrated corporate, markets, financial services and consumer credit regulator" (ASIC 2023, 9)	1 690	2011-09-30	2024-03-14	JSON	—
Financial Conduct Authority	FCA	UK	"independent financial regulator" (FCA 2023, 18)	13 369	2000-01-01	2024-03-21	—	—
Securities and Exchange Commission	SEC	USA	"protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation" (SEC 2024)	1 584	—	—	—	—
Central Bank of Ireland	—	Ireland	"maintaining monetary and financial stability" (Central Bank of Ireland 2023, 2)	362	2016-03-04	2024-03-26	—	—
Ontario Securities Commission	OSC	Ontario, Canada	"regulates Ontario's capital markets by making rules that have the force of law" (OSC 2024)	802	2008-12-09	2024-03-25	—	—
Monetary Authority of Singapore	MAS	Singapore	"central bank and integrated financial regulator" (MAS 2024)	96	2022-01-07	2024-03-22	—	—
International Organization of Securities Commissions	IOSCO	Global	"international body that brings together the world's securities regulators" (IOSCO 2024a)	24 336	2010-08-06	2024-01-31	—	—

The alerts published on the regulators' web sites are aimed at human readers. However, to use the alerts for automated cybersecurity purposes requires that the data is made available in formats amenable to computer programs. Table 1 also shows an overview of the characteristics of data provision at the selected portals. None of the portals provide an Application Programming Interface (API) to enable simple machine-readable access to the data. Only the FMA and Moneysmart provide a structured downloadable file.

The FCA has both the largest number and the oldest alerts in our sample of regulators (dating back to 2000). However, the counts in Table 1 should only be viewed as estimates due to the difficulty of reliably extracting information where there is no defined data feed. The SEC doesn't attach dates to their alerts and not all of the alerts in the member portals are found at IOSCO (e.g. alerts before 2011-01-24 from the Ontario Securities Commission). In the next sections we focus on the two regulators (the FMA and Moneysmart) who do provide data and then consider the global perspective.

3.1 New Zealand: data provision from the FMA

The format used for data representation of the alerts varies between regulators and is also different to the aggregated presentation at IOSCO. For example, the FMA alert for *NZX Wealth Investments* has three partially overlapping representations: the FMA alert list entry, a row in a CSV[1] download option from the FMA website and the IOSCO portal entry. Similar inconsistencies can be observed with the alerts at the other portals in Table 1.

The FMA CSV file has 13 fields including: *Entity Name, Date, Content, Trading Name, Website, Email* and *Tags*. However, only four fields (*Entity Name, Date, Content* and *Tags*) contain any values. For the *NZX Wealth Investments* entry the *Entity Name* is `NZX Wealth Investments - Imposter website` and the *Tags* field is `Imposter website, Suspected scam`. The *Content* field mainly contains a textual description of the alert but also some structured text: a domain (labelled as `Website`) and an `Email`. Parsing this CSV file is therefore awkward and it seems to have been published without an expectation of being re-used in a systematic manner. In addition, the *Content* field contains many examples of 'control characters' for newlines (`\n`) and HTML entity codes (` `): these technical markup characters should not be present in plain text content and are a failure of data quality control.

The corresponding IOSCO portal entry has seven fields: *Company, Regulator, Jurisdication Date, Link, Subject* and *Comments*. The IOSCO *Comments* field is broadly similar to the FMA *Content* field, the FMA *Tags* field is not represented at all and the IOSCO *Subject* field lists three new comments (e.g. "Regarding registration of issuance, offer or sale of securities/derivatives, and reporting requirements").

3.2 Australia: data provision at Moneysmart

The only other portal from Table 1 with data provision is *Moneysmart* published by the *Australian Securities and Investments Commission* (ASIC), where the alert list is a JSON file.[2] The JSON format is designed for processing by a computer rather than

Table 2 Most frequent domains and terms in 1503 URLs from the Moneysmart alerting data (at 2024-02-01)

Domains	Count	Terms	Count
.com	991	capital	90
.org	66	trade	74
.net	42	fx	57
.us	29	group	47
.io	19	global	46
.uk	11	invest	46
.au	11	trading	38
.co	7	market	37
.hk	5	inc	34
.eu	5	financial	28

reading by a human. This data shows better quality than the FMA file: with websites and emails in clearly defined fields. The Moneysmart JSON data contains 21 data fields. However, only three fields contain data in each entry—*dateUpdated*, *Name*, and *investorAlertCategory*—as such the remaining data fields are classified as optional. Inspection of the *dateUpdated* field suggests that there is a cut-off date for reports with many entries labelled with the same date (2019-08-23). These inconsistencies in dates present a challenge for analysing temporal trends but would not affect using the data to protect consumers. This legacy issue is also observed in the *investorAlertCategory* field, where the labels to categorize each report are: `Unlicensed (Legacy)`, `Unlicensed` and `Imposter`.

Although it is possible to 'scrape' content from the web presentation of most of the investor alerting portals, this approach tends to produce lower quality results than a dedicated API or published data file (Dogucu and Çetinkaya Rundel 2021). Moneysmart is the best exemplar of quality data publishing from the portals in Table 1 and illustrates the value in the alerts. Table 2 shows the most frequent top-level domains and terms from the URLs in the Moneysmart alerts.

The `.au` domain for Australia is only the joint sixth most frequent domain in the alerts. The presence of domains from other areas (`.uk`, `.hk` and `.eu`) partially reflects the international nature of cybersecurity threats. However, outside the USA (where the `.us` domain is rarely used for finance), country-specific domains are common for financial institutions (e.g. `anz.com.au`, `bnz.co.nz`, `barclays.co.uk`). A website offering an investment to Australian consumers from a `.hk` domain, for example, might be seen as unusual. The frequent terms extracted from the URLs reflect attempts to legitimize a fraudulent entity through naming by using terms from the financial sector. The use of 'inc' (incorporated) may be used to suggest some legal 'incorporation' process has been completed (e.g. `www.globalmanagementinc.com`). This kind of analysis might be able to inform services that monitor the safety of websites: for example, using term analysis of URLs together with territory requirements (Trimble 2018).

3.3 Global data provision

The other regulators in Table 1 do not provide a data source for their alerts. The FCA, SEC, Ontario Securities Commission and Central Bank of Ireland each provide an RSS (Really Simple Syndication) feed (Hammersley 2003) that includes alerts. All but Ontario add other content, such as press releases and investor education, into this data. Although the XML of an RSS feed can provide structured data these feeds are, in practice, not organized enough to provide an API-like service. The main impression from inspecting the portals listed in Table 1 is one of inconsistency. Useful operations such as sorting, filtering and searching are all made difficult by the mixing of content and lack of structure. Whilst it is possible to extract structured data from these websites (through scraping) the process is unreliable and inefficient.

The global alert aggregation at IOSCO is presented as web content with no data file or API. IOSCO's web alerts contain seven elements, out of which five appear to be mandatory. These are *Company*, *Regulator*, *Jurisdiction*, *Date*, and *Link*. The *Company* field appears to be associated to subject of the report. There does not appear to be a predefined format or structure to this field, as the subject can be presented in various formats, such as domains, company names or emails. The *Regulator* field is the name of jurisdiction's official reporting regulator. For example, the jurisdiction of New Zealand has the FMA as their reporting regulator. As such, the *Regulator* and *Jurisdiction* fields follow a list of jurisdictions and regulators derived from IOSCO membership. The *Link* field provides a URL back to the original regulator's website. However, for some older alerts, these links often point to web pages which are no longer accessible.

Investor alerting reflects considerable knowledge work undertaken by financial regulators that is continually published to their respective websites. However, these alerts are inconsistent with each other and are inconsistently aggregated by IOSCO. The estimate of alert counts in Table 1 gives an overview of the available data, but each alert is a product of the environment of the local regulator. A similar set of evidence may produce an alert in one country but not in another. Even similar alerts may be reported with different levels of detail in different jurisdictions: varying from just a URL to metadata tags to several paragraphs of background information. However, a URL is present in almost all alerts. Most regulators we inspected did not publish their alerts as data: so little of their work can be easily used by computers. The only two data publishers, the FMA and Moneysmart, provide minimal metadata: with no description of their data fields and no clear licensing information.

Zetzsche et al. (2019) highlights the differences in legal environments in relation to cryptocurrency but also notes that the required resources to regulate "may be disproportional to the local impact". Consequently, alerts may partially reflect the policy priorities of financial regulators. Longitudinal analysis is also complicated as the threats, laws, policies, reporting practices and regulator resources will change over time. All of these issues are a challenge to the analysis and aggregation of this data: we have not attempted any textual qualitative analysis of the alerts and have only provided estimates of the number of alerts. Despite these challenges the value of the alerts for cybersecurity is clear. The URLs in the alerts will not represent all dangerous websites, but those reported have all been flagged as dangerous by financial regulators.

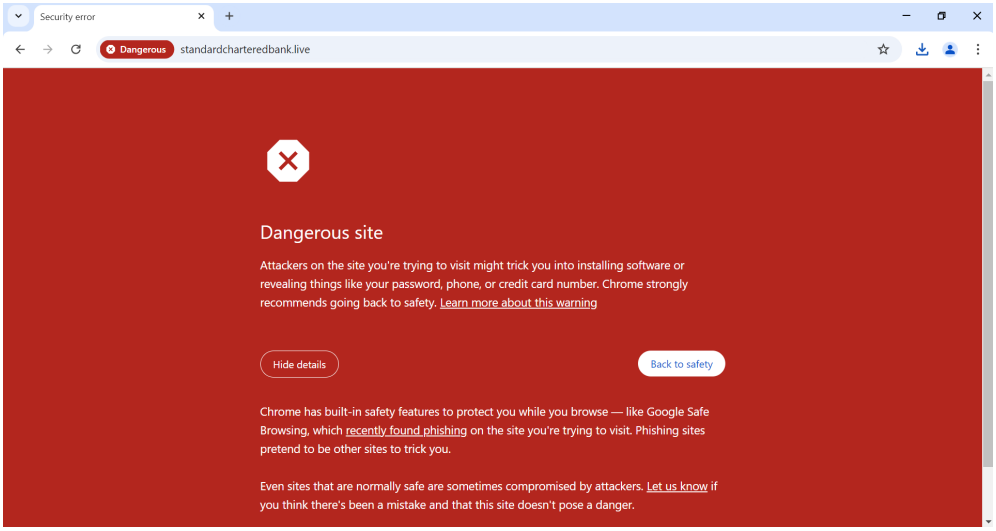

Fig. 2 The Chrome warning message for a website detected by the Google Safe Browsing service (`standardcharteredbank.live`)

In the following section we explore whether these dangerous websites are detected by services designed to protect consumers.

4 Safe Browsing Services

Phishing websites are a common element of the investor alerts. Web browsers such as Google Chrome and Microsoft Edge include specific features to protect users from dangerous websites (Chrome's service is *Safe Browsing-Enhanced protection* and in Edge it is *MS Defender SmartScreen*) (Oest et al. 2019). URLs are checked against known lists of dangerous sites and, if found, the browser presents a prominent warning to the user. These "blacklists are a user's main and at times only technical line of defense against phishing" (Oest et al. 2019).

A small exploratory study was performed to assess whether the websites reported by the regulators were detected by safe browsing services. We examined alerts published in August-September 2024 by the FMA, MoneySmart and the FCA. From the alerts that mentioned specific websites we extracted 13 URLs from each source. These 39 URLs were manually tested in Chrome and Edge with their safe browsing services active. Several URLs were not active during testing and others were misconfigured: this might be reflective of a focus on the first few "golden hours" of an attack Oest et al. (2020) or a general lack of quality web publishing among attackers. When a website is recognised by these in-browser safety services they display a prominent warning message to the user (Figure 2): the study counted the presence or absence of these warning messages. Details of all the tests in this section are provided in the Supplementary Information.

37 of the 39 URLs in our sample were not detected by either browser. One URL (`standardcharteredbank.live`) was not active during testing but Chrome still presented a warning page (Figure 2); whereas Edge just displayed a dead site message. This behaviour is expected as the browser checks the URL against an exclusion list before visiting the site. Another URL (`https://www.revolutwealth.net/trading`) produced a warning from Edge but not from Chrome. These two URLs were the only ones to trigger a warning alert from either browser over a month of testing: notably both were imposter sites of major financial institutions.

The striking implication is that Google and Microsoft are not using investor alerts from major financial regulators to inform their safe browsing services. A prior study on phishing websites (Oest et al. 2019) used the crowd-sourced collection of dangerous URLs at *Phishtank* PhishTank (2024) in addition to the commercial safe browsing services. Our sample of 39 URLs was manually tested for presence in the *Phishtank* collection: none were found.

We also tested our sample URLs with *CheckNetsafe AntiScam* (CheckNetsafe 2024): a service from *Netsafe NZ* who are "New Zealand's independent, non-profit online safety organisation" (Netsafe 2024). *CheckNetsafe* runs 16 tests on a given URL, utilising external services for quality indicators including: SSL configuration, presence in exclusion lists (such as APWG APWG (2024)) and evaluations at review-based sites (such as *Trustpilot* (Trustpilot 2024)). The test services were all international apart from *CERT NZ*: the Computer Emergency Response Team of the National Cyber Security Centre of New Zealand (NCSC 2024). For each URL's 16 test results *CheckNetsafe* reported a result of *positive*, *negative* (i.e. dangerous) or *neutral*; a textual summary assessment is also provided (e.g. "We think the website is likely to be legitimate").

Evaluation of the 39 URLs with the 16 tests is a potential 624 data points. However, three URLs produced no output and one test only assessed website encryption: excluding those leaves 540 meaningful results from 36 URLs. Of these, 46% were *positive*, 45% *neutral* and only 9% *negative* (i.e. dangerous). The most common textual summary (23 out of 36) was "This site may not be safe to use". Eight summaries indicated that the tested URL was "likely to be legitimate" or "possibly legit".

Only two of the 16 testing services used by *CheckNetsafe* showed any substantial accuracy from the 36 URLs: Scamadviser (ScamAdviser 2024) and IPQS (IPQualityScore 2024), with 25 and 11 hits respectively. Eight of the testing services reported no *negative* results at all. Although one third of the sample URLs were from alerts at the New Zealand FMA, the CERT NZ results were all *neutral*. Although the tests were reported separately, some of the testing services use data from each other (e.g. *Scamadviser* uses input from *Trustpilot* and *Sitejabber* (Sitejabber 2024)) so their results are not independent.

All of the URLs in our exploratory sample represent websites that financial regulators have recently assessed to be dangerous: ideally, each one of them would be blocked by web browsers and detected by cybersecurity safety services. The low rates of blocking and detection we observed represent unnecessary risks to consumers and many missed opportunities to prevent financial scams.

5 Discussion

Our two main findings are that:

- the publishing of investor alerts is partial, inconsistent and in formats that make computational re-use difficult
- the URLs in investor alerts are largely not detected by safe browsing services

Only two of the investor portals in Table 1 publish a data version of their warnings. However, the data published by the FMA and Moneysmart lacks both a textual description of the data fields and any licensing information. A good description of the data, in a data dictionary, is an important element of successful data re-use (Xiao et al. 2023). Best practice for data sharing is also to provide explicit labels with information on usage permissions (Jacobsen et al. 2020; Quarati 2023). A public domain label would minimise any copyright concerns by other parties who might want to use the data.

IOSCO aggregates alerts from many jurisdictions but the lack of a common schema raises barriers to re-use.[3] The work of harmonisation is distributed to potential users, rather than completed once during aggregation. The lack of common structure in most of the alerting feeds also implies the use of more complex text mining techniques (Ignaczak et al. 2021) to realize the true value of the content. The absence of a global standard is likely a contributory factor to the absence of a machine-readable data feed of investor alerts.

From the regulators in Table 1, only MoneySmart in Australia is providing good quality data in an appropriate format. As the regulators are legally constituted in their jurisdictions, this level of provision can be viewed as a widespread failure of the ideals of open government data (Quarati 2023). A possible interpretation is that the financial regulators view their alerting efforts as part of investor education, rather than as valuable data for computer systems. The gap between the detection of a dangerous website and its inclusion in the lists of safe browsing services is a window of opportunity for consumers to become victims of investment scams. In many situations this gap is measured in hours (Oest et al. 2019), however most of the URLs in investor alerts never seem to reach the services which could protect users.

The URLs that are reported by the regulators are largely not detected by the main in-browser services or several other cybersecurity tools. We suspect that the poor data publishing of the regulators, outlined above, is a major factor in this lack of detection. On one side we have financial regulators, on the other major computing corporations—and seemingly no cooperation between them.

The only two URLs in our sample that were detected by Chrome or Edge contained the brand names of large financial institutions (*Revolut* and *Standard Chartered*). This result is reminiscent of Oest et al.'s observation "that only URLs containing brand names were quicker to be blacklisted than others" (Oest et al. 2019). Although these were very different studies it may be that large financial brands are treated as special cases.

The "inability of many people to recognize the red flags of fraud" Kieffer and Mottola (2017) highlights the potential utility of an external assessment of a website. The current browser warnings are visually striking and likely to be effective in

informing users of the risks (Reeder et al. 2018). A large scale study of phishing campaigns supports the view that these "browser-based phishing warnings are clearly an effective mitigation overall" (Oest et al. 2020). Burke et al. (2022) suggest that educational interventions can contribute to reducing users vulnerability to financial scam. Browser-based warnings could play a similar role to the "source credibility" prompt used in their study.

Current warnings from Google and Microsoft do not identify the underlying reason why a user has been interrupted in trying to visit a website. These warnings may be even more effective if the browser could direct users to the original investor alert on the website of the financial regulator. In addition to browser-based warnings, a simple list of dangerous URLs could also be used in the ranking of search-engine results, online advertising (especially adverts alongside search-engine results) and in other defensive networking technologies (e.g. protective DNS (Rodríguez et al. 2023)). For some users it may also be possible to block websites at their internet service provider, although this depends on the specific configuration of their networking access.

A limitation of this exploratory study is that our small sample of URLs was manually extracted and only tested over two months in 2024. All of the URLs reported as dangerous should be continually monitored for detection via both browser and independent safety services.

5.1 Recommendations

Based on our investigation, we provide some recommendations. The discussion below follows the data from reporting to potentially intercepting a financial crime and addresses the role of regulators in making their work re-usable and actionable.

A typical scam begins when a scammer creates a website for an investment scam. Victims are then targeted, either actively or passively. Eventually, the scam is reported to a regulator. After carrying out an investigation, the regulator publishes an entry on the scam to their alert web portal.

Our investigation has found that most regulators do not publish this data in a machine-readable format. The portals are designed for human readers visiting the websites, which limits the utility of the data. If this data was machine-readable, it could be directly parsed and utilised by other scam-prevention mechanisms–increasing its utility. For example, such data feeds could be used in browsers or directly in the apps of financial institutions. The lack of structured data means that the best that can be done is to direct the user to an alerting portal and completely rely on the user making the right use of the alerting portal. The lack of machine-readable data has also hindered data collection and analysis in this area, which would be valuable in gaining further insight into scammer behaviour.

The FMA portal has poor data quality, with empty data fields and several values conflated in a single field. This creates a number of challenges for anyone wanting to utilise this data. We recommend that all alert data should be well-structured and consistent: with appropriate use of controlled vocabularies and free-text content to enable broad uptake. For data that is in public domain and for the public good, it is important that there is clarity about what the data fields mean and how the data can

be used. We recommend that alert data should have an associated data dictionary and an explicit licensing statement for open data (Quarati 2023).

Beyond providing the alert data, the regulators should also test the usefulness of their data and their alerting mechanisms. Placing themselves in the position of consumer would enable them to see whether their alerts are having a practical effect in reducing harm. Most regulators currently do not seem to go beyond presenting the data in the portal. However, this high-quality data could be used proactively for scam-prevention. Victims interact with scam websites through browsers and preventative measures in the browser have the potential to reduce harm. While browser developers use data about malicious URLs from various other repositories to warn users about malicious websites, our study indicates the data in investor alert portals is not being used. Financial regulators and IOSCO should coordinate with browser developers to ensure alerting data is included in safe browsing services.

In Section 3 we noted the inconsistent nature of alerting across different jurisdictions. These variations have implications for the global safety services provided by browser developers. Although one regulator may warn about a financial website being unlicensed in their country, that site could be legal and licensed elsewhere. A web browser using a global warning list may interrupt users when accessing legal services. The provision of country-specific warnings is technically feasible but adds to the complexity of the service. The regulators and IOSCO should coordinate with browser developers on the best way to provide warnings to users that balance safety whilst respecting jurisdictional differences. As with many aspects of security there is a balance to be struck between protection and inconvenience.

6 Conclusion

The provision of alerts to investors is a valuable service that has the potential to reduce the incidence of financial crimes. The main contributions of this paper are to:

- document the inconsistent and poor quality data publishing of many financial regulators: including the international body IOSCO
- show that computing corporations are not using a valuable source of data on dangerous websites
- highlight that consumers could be better protected by closing the informational gap between regulators and browser developers

Our answer to the question in the paper's Introduction is: yes, with some difficulty with current practice. We believe that improved data publication practices could be used to prevent many more consumers from becoming victims. Existing publication channels fail to effectively disseminate the detailed knowledge work undertaken by IOSCO members to assess cybersecurity risks to the public.

The alerts show a variety of financial dangers but most of them involve a customer transferring money to a bad actor after interacting with a dangerous website. These APP transactions are a challenge for banking systems to address as customer 'authorisation' has more in common with legitimate transactions than other forms of financial crime on the internet (Maher 2021). The safe browsing services provided by major

computer corporations are a supplementary channel where investor alerts could be applied to address an APP scam before it ever reaches the banking system. However, possible actions in the web browser should always be a complement, not a substitute, to other defences within the payments ecosystem (Doeland 2019; Akesson et al. 2023).

The lack of coordination between the regulators and the computing industry represents a missed opportunity to impede APP scams involving websites. We can't be sure that better collaboration will be successful, but effective data sharing should be regarded as a base level of best practice. Indeed, failing to provide these high-value alerts in a useful format could be regarded as negligence on the part of the financial regulators. The exception is Australia: where the data publication at Moneysmart is a good model for other jurisdictions to follow. However, the global nature of cybersecurity threats needs to be matched by a coordinated global response from the financial regulators. IOSCO has been involved in considerable coordination and standardisation work in the financial sector (Marcacci 2023) but has not provided an aggregated data feed to enable improved cybersecurity for users.

Future work could examine the content of investor alerts in greater detail than we have covered in this paper. This could include both their topics and the alerts that were outside our scope. It would also be valuable to collect data on the awareness and utility of the investor alerts from both regulators and investors. Do consumers consult the warnings before engaging with financial service providers? Were victims aware of these alerting portals before they were scammed? The international nature of financial scams requires both research and practice with a global scope. Analysis could extend to alerting in a wider range of countries and in languages other than English. Additionally, the websites identified in investor alerts could be continually tested against safety services to ensure that the value of the financial regulators' work is realized in practical protections for users.

Notes

1. Comma-separated values (CSV) is a common data format that can be read by spreadsheets such as Microsoft Excel.
2. JSON (JavaScript Object Notation) is a commonly used format for data representation by web applications.
3. The Canadian Securities Administrators (`https://www.securities-administrators.ca`) also aggregates alerts from Canada's provinces and territories in a similar manner to IOSCO; although there is no national machine-readable data feed.

Supplementary information. Supplementary information, including data and code, is available at:
https://doi.org/10.17605/OSF.IO/QN46F

References

Abraham, J., S. Rogers, C. Njoki, and J. Greening. 2024. *The State of Scams in New Zealand 2024*, Global Anti-Scam Alliance. https://resource.netsafe.org.nz/State-of-Scams-Report-New-Zealand---2024-Final.pdf Accessed 9 December 2024.

Akesson, J., J. Gathergood, and E. Quispe-Torreblanca. 2023. *Preventing Payments Fraud in the FinTech Era: New Evidence from a Behavioural Experiment*. Discussion Paper No. 2023-08, Centre for Decision Research and Experimental Economics, University of Nottingham, UK. https://doi.org/10.2139/ssrn.4532757

APWG. 2024. APWG — Unifying The Global Response To Cybercrime. https://apwg.org Accessed 9 December 2024.

ASIC. 2023. *Australian Securities and Investments Commission Annual Report 2022–23*. https://download.asic.gov.au/media/b3zf3or3/asic-annual-report-2022-23_full.pdf Accessed 9 December 2024.

Bank of New Zealand. 2024. Recognising scams - BNZ. https://www.bnz.co.nz/about-us/online-security/recognising-scams Accessed 9 December 2024.

Braithwaite, J. 2024. 'Authorized Push Payment' Bank Fraud: What does an effective regulatory response look like? *Journal of Financial Regulation 10*(2): 174–193. https://doi.org/10.1093/jfr/fjae006 .

Burke, J., C. Kieffer, G. Mottola, and F. Perez-Arce. 2022. Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization* 198: 250–266. https://doi.org/10.1016/j.jebo.2022.03.028 .

Central Bank of Ireland. 2023. *Central Bank of Ireland Annual Report 2022 & Annual Performance Statement 2022 - 2023*. https://www.centralbank.ie/docs/default-source/publications/corporate-reports/annual-reports/annual-report-2022-and-annual-performance-statement-2022-2023.pdf Accessed 9 December 2024.

CheckNetsafe. 2024. CheckNetsafe.nz — Check if a Website is a Scam or a Fraud. https://checknetsafe.nz Accessed 9 December 2024.

Dahlgreen, J. 2023. Catastrophic fraud loss lies where it falls? Push payment scams and the bank's duty of care to its customer. *Journal of Financial Crime 30*(6): 1845–1852. https://doi.org/10.1108/JFC-10-2021-0223 .

Dobrauz-Saldapenna, G. and U. Klebeck. 2019. Initial coin offering—legal and regulatory challenges of crossing the borders. *The Journal of Alternative Investments 21*(4): 81–94. https://doi.org/10.3905/jai.2019.21.4.081 .

Doeland, M. 2019. How to keep payments safe and secure in a changing world. *Journal of Payments Strategy & Systems 13*(2): 132–137. https://doi.org/10.69554/fslk7337 .

Dogucu, M. and M. Çetinkaya Rundel. 2021. Web scraping in the statistics and data science curriculum: Challenges and opportunities. *Journal of Statistics and Data Science Education 29*(sup1): S112–S122. https://doi.org/10.1080/10691898.2020.

1787116 .

FCA. 2023. *Financial Conduct Authority Annual Report and Accounts 2022/23*. https://www.fca.org.uk/publication/annual-reports/annual-report-2022-23.pdf Accessed 9 December 2024.

FMA. 2016. *FMA Regulatory Response Guidelines*. https://www.fma.govt.nz/assets/Policies/160824-Regulatory-response-guidelines-policy.pdf Accessed 9 December 2024.

FMA. 2023. *Financial Markets Authority Annual Report 2022/23*. https://www.fma.govt.nz/assets/Corporate-Publications/FMA-2023-Annual-Report.pdf Accessed 9 December 2024.

FMA. 2024. Real life scam stories. Financial Markets Authority, New Zealand. https://www.fma.govt.nz/scams/real-life-scam-stories/ Accessed 9 December 2024.

Hammersley, B. 2003. *Content Syndication with RSS*. Sebastopol, CA: O'Reilly.

Ignaczak, L., G. Goldschmidt, C.A.D. Costa, and R.D.R. Righi. 2021. Text mining in cybersecurity: A systematic literature review. *ACM Computing Surveys 54*(7): Article 140. https://doi.org/10.1145/3462477 .

IOSCO. 2024a. About IOSCO. IOSCO. https://www.iosco.org/v2/about/?subsection=about_iosco Accessed 9 December 2024.

IOSCO. 2024b. Investor Protection. IOSCO. https://www.iosco.org/v2/investor_protection/?subsection=investor_alerts_portal Accessed 28 January 2025.

IPQualityScore. 2024. Fraud Detection, Bot Detection & IP Address Intelligence — Detect Fraud With IPQS. https://www.ipqualityscore.com Accessed 9 December 2024.

Jacobsen, A., R. de Miranda Azevedo, N. Juty, D. Batista, S. Coles, R. Cornet, M. Courtot, M. Crosas, M. Dumontier, C.T. Evelo, C. Goble, G. Guizzardi, K.K. Hansen, A. Hasnain, K. Hettne, J. Heringa, R.W. Hooft, M. Imming, K.G. Jeffery, R. Kaliyaperumal, M.G. Kersloot, C.R. Kirkpatrick, T. Kuhn, I. Labastida, B. Magagna, P. McQuilton, N. Meyers, A. Montesanti, M. van Reisen, P. Rocca-Serra, R. Pergl, S.A. Sansone, L.O.B. da Silva Santos, J. Schneider, G. Strawn, M. Thompson, A. Waagmeester, T. Weigel, M.D. Wilkinson, E.L. Willighagen, P. Wittenburg, M. Roos, B. Mons, and E. Schultes. 2020. FAIR Principles: Interpretations and Implementation Considerations. *Data Intelligence 2*(1-2): 10–29. https://doi.org/10.1162/dint_r_00024 .

Kadoya, Y., M.S.R. Khan, and T. Yamane. 2020. The rising phenomenon of financial scams: evidence from Japan. *Journal of Financial Crime 27*(2): 387–396. https://doi.org/10.1108/JFC-05-2019-0057 .

Kieffer, C. and G. Mottola. 2017. Understanding and combating investment fraud, In *Financial Decision Making and Retirement Security in an Aging World*, eds. Mitchell, O.S., P.B. Hammond, and S.P. Utkus, 185–212. Oxford: Oxford University Press.

Maher, R. 2021. A critical analysis of recent efforts in the United Kingdom to tackle authorised push payment scams and the impact on the bank-customer relationship. *Trinity College Law Review* 24: 134–145 .

Marcacci, A. 2023. *Transnational Securities Regulation: How it Works, Who Shapes it*. Cham: Springer.

MAS. 2024. Who we are - Monetary Authority of Singapore. https://www.mas.gov.sg/who-we-are Accessed 9 December 2024.

Moneysmart. 2024. Investor alert list - Moneysmart.gov.au. https://moneysmart.gov.au/check-and-report-scams/investor-alert-list Accessed 9 December 2024.

NCSC. 2024. National Cyber Security Centre, New Zealand. https://www.ncsc.govt.nz/ Accessed 9 December 2024.

Netsafe. 2024. Netsafe New Zealand. https://netsafe.org.nz/netsafe Accessed 9 December 2024.

Oest, A., Y. Safaei, A. Doupé, G.J. Ahn, B. Wardman, and K. Tyers 2019. Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. In *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP 2019)*, pp. 1344–1361. https://doi.org/10.1109/SP.2019.00049

Oest, A., P. Zhang, B. Wardman, E. Nunes, J. Burgis, A. Zand, K. Thomas, A. Doupé, and G.J. Ahn 2020. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, pp. 361–377. USENIX Association.

OSC. 2024. About us — Ontario Securities Commission. https://www.osc.ca/en/about-us Accessed 9 December 2024.

PhishTank. 2024. PhishTank — Join the fight against phishing. https://www.bnz.co.nz/about-us/online-security/recognising-scams Accessed 9 December 2024.

Quarati, A. 2023. Open government data: Usage trends and metadata quality. *Journal of Information Science 49*(4): 887–910. https://doi.org/10.1177/01655515211027775 .

Reeder, R.W., A.P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman 2018. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI*

2018), pp. Paper No.: 512, 1–13. ACM.

Reurink, A. 2018. Financial fraud: a literature review. *Journal of Economic Surveys 32*(5): 1292–1325. https://doi.org/10.1111/joes.12294 .

Rodríguez, E., R. Anghel, S. Parkin, M. van Eeten, and C. Gañán 2023. Two sides of the shield: Understanding protective DNS adoption factors. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*, pp. 3135–3152. USENIX Association.

Rutledge, G.P. 2022. Financial crime: the regulator's perspective, In *A Research Agenda for Financial Crime*, ed. Rider, B., 105–124. Cheltenham, UK: Edward Elgar Publishing.

ScamAdviser. 2024. Scamadviser.com — check a website for risk. https://www.scamadviser.com Accessed 9 December 2024.

SEC. 2024. SEC.gov — Mission. Securities and Exchange Commission. https://www.sec.gov/about/mission Accessed 9 December 2024.

Sitejabber. 2024. Check Ratings of Businesses, Read Reviews & Buy - Sitejabber. https://www.sitejabber.com Accessed 9 December 2024.

Sood, P. and P. Bhushan. 2020. A structured review and theme analysis of financial frauds in the banking industry. *Asian Journal of Business Ethics* 9: 305–321. https://doi.org/10.1007/s13520-020-00111-w .

Trimble, M. 2018. Territorialization of the internet domain name system. *Pepperdine Law Review* 45: 623–684 .

Trustpilot. 2024. Trustpilot reviews: Experience the power of customer reviews. https://www.trustpilot.com Accessed 9 December 2024.

Xiao, F., Y. Chi, and D. He. 2023. Promoting data use through understanding user behaviors: A model for human open government data interaction. *Journal of the Association for Information Science and Technology 74*(13): 1498–1514. https://doi.org/10.1002/asi.24831 .

Zetzsche, D.A., R.P. Buckley, D.W. Arner, and L. Föhr. 2019. The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators. *Harvard International Law Journal 60*(2): 267–315 .