Note : Below are extracts from online content issued by FraudSMART.ie, an initiative of the Banking & Payments Federation Ireland (BPFI), (10th August 2022) and the World Economic Forum (March 1st, 2022), both as referenced below.

Text message scams cost victims an average of €1,700 in the first half of 2022.

New FraudSMART campaign warns consumers and business to be on high alert to impersonation scams as fraudsters seek to take advantage of the transition of hundreds of thousands of bank accounts in the coming months

FraudSMART.ie, an initiative of the Banking & Payments Federation Ireland (BPFI) reports on the significant increases in scamming and subsequent financial losses to individuals and businesses alike. This is of great significance to the team at Seaspray Private and our clients, supporting our rationale for continued investment in cyber security and reinforcing our commitment to ESG(Economic Social and Governance) investment strategies and to building a culture of Corporate Social Responsibility (CSR).

According to Fraudsmart.ie/BPFI (2022), its members have seen text message scams almost double in the first half of this year compared to the same period last year :

> Victims of text message scams or 'smishing' were tricked out of an average of €1,700 during the first half of this year. The figures also show that over the same period businesses were conned out of an average of €14,000 due to invoice fraud. The figures come as FraudSMART launches a new information and awareness campaign urging both consumers and business to be on high alert for impersonation type scams as thousands of bank customers prepare to move their bank accounts over the coming months due to the exit of Ulster Bank and KBC from the Irish market.
>
> Niamh Davenport, Head of Financial BPFI and FraudSMART lead said: "Fraudsters are experts at taking advantage of changing situations to commit fraud and with two retail banks leaving the Irish market and hundreds of thousands of personal and businesses customers moving bank accounts FraudSMART members are anticipating we may see a rise in impersonation fraud attempts which will be based around the process of verifying and updating bank account details.

> In response we have this week launched an information and awareness campaign urging consumer and business to be on high alert in the coming weeks and months to fake text messages, emails or calls pretending to come from trusted organisations such as your bank, utility company, streaming service, mobile provider or even your employers HR Department."
>
> (FraudSMART.ie/BPFI, 2022)

Sarnek and Dolan (2022) make a strong argument that "For businesses, putting cybersecurity at the heart of ESG strategies is vital to demonstrate good governance….and that cyber attacks present a huge risk to the value of companies and ultimately the stability of society. They conclude that "companies need to start managing cybersecurity as part of their ESG governance strategy, rather than relying on insurance."

The Seaspray Private investment strategy follows this thought process and matches its clients' aspirations. We have a strong conviction that cyber security will play an ever increasing role in the coming decade as the world's economies continue to digitize. We can see this in the proliferation of cyberattacks in recent years, both on businesses and individuals, and as part of this year's geopolitical instability. Cyber criminals may be getting smarter in their methods of attack, but so too are cyber defence firms and technologies, bolstered by rising investments from both the private and public sectors.

In relation to the current scams in the Irish market, FraudSMART (2022), goes on to highlight how fake texts are targeting personal customers of the banks exiting the market, who are looking to set up new accounts with an alternative bank:

> For personal customers we expect fraudsters will use this account transition period to obtain personal information through the guise of a problem with a customer's new account set-up or switch. We are warning consumers to be on the lookout for text messages that flag fraud on your bank account or impending cancelation of your salary, standing orders, or direct debits to utilities and which then go on to ask for personal information or account details. We are aware that fraudsters have recently started to follow up these texts with a phone call from a number that appears to be your bank.
>
> (FraudSMART.ie/BPFI, 2022)

FraudSMART.ie(2022) reports that the risk of cyber attack is also a stark reality currently, for Irish business:

> Niamh Davenport also outlined the increased risk for business: "We are issuing a serious warning to businesses who are particularly vulnerable in the current environment. With over 70,000 businesses due to move their accounts there is a greater threat than ever of invoice fraud the effects of which can be devastating particularly for SMEs. Already this year FraudSMART members have seen over 100 cases of invoice fraud with businesses suffering average losses of €14k but which can range up to €50k. Invoice fraud involves a fraudster notifying your company that supplier payment details have changed and providing alternative details in order to defraud you. The fraudster could be claiming to be from your company's genuine supplier, or even be posing as a member of your own firm. With so many businesses who will now be legitimately changing their account details, this provides the perfect opportunity for criminals to take advantage."
>
> Niamh Davenport concluded: "As we launch our campaign this week which people will hear on the radio as well as see online and via social media, our key message, be it to consumers or business, is to take your time, never click on links in texts or emails and verify any communication, text or email, and do so by using contact details you have on file, the back of your bank card or via a website directly."
>
> (FraudSMART.ie/BPFI, 2022)

Key advice for consumers re impersonation scams

- Do not respond to messages with personal information.
- Do not click on links or follow directions from somebody on a call without verifying first.
- A bank will never text/email/phone looking for personal information.
- Contact your bank/service provider/employer provider directly.
- Never use contact details from a text message, always independently verify.
- Always double check before clicking links or attachments in random or unexpected emails or texts and never give away security details such as PINs or passwords to anyone.

Key advice for business to prevent invoice fraud

- Verify the fundamental banking changes by contacting a known contact in the company directly, use contact details held on record or a contact number on the company's website.
- Have a verification process in place before changing saved bank account details of your suppliers or service providers.
- Inform employees of this fraud so they are alert to it and can avoid it. Practical advice for employees:

- The first contact may inform you of a change in bank account details but not request payment. This ensures that all future payments are sent to the new account.
- Do not to use the contact details on the letter/email requesting the change as these could be fraudulent.
- Look out for different contact numbers and email addresses for the company as these may differ from those recorded on previous correspondence.
- Consider setting up designated Single Points of Contact with companies to whom you make regular payments.
- Fraudsters can change an email address to make it look like it has come from someone you email regularly. Look out for different contact numbers and/or a slight change in the email address e.g. .com instead of .ie as these may differ from previous correspondence.

References

FraudSMART.ie/Banking & Payments Federation Ireland (BPFI) (2022) '*Text message scams cost victims average of €1,700 in H1 2022 with businesses suffering average losses of €14,000 due to invoice fraud*'. Dublin. Available at: https://www.fraudsmart.ie/2022/08/10/text-message-scams-cost-victims-average-of-e1700-in-h1-2022-with-businesses-suffering-average-losses-of-e14000-due-to-invoice-fraud/ . [Accessed 15 August 2022].

Anna Sarnek & Christina Dolan , World Economic Forum, March 1st 2022 , *"Cybersecurity is an environmental, social and governance issue. Here's why"*.(Accessed 15th August 2022).Available at :: https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/