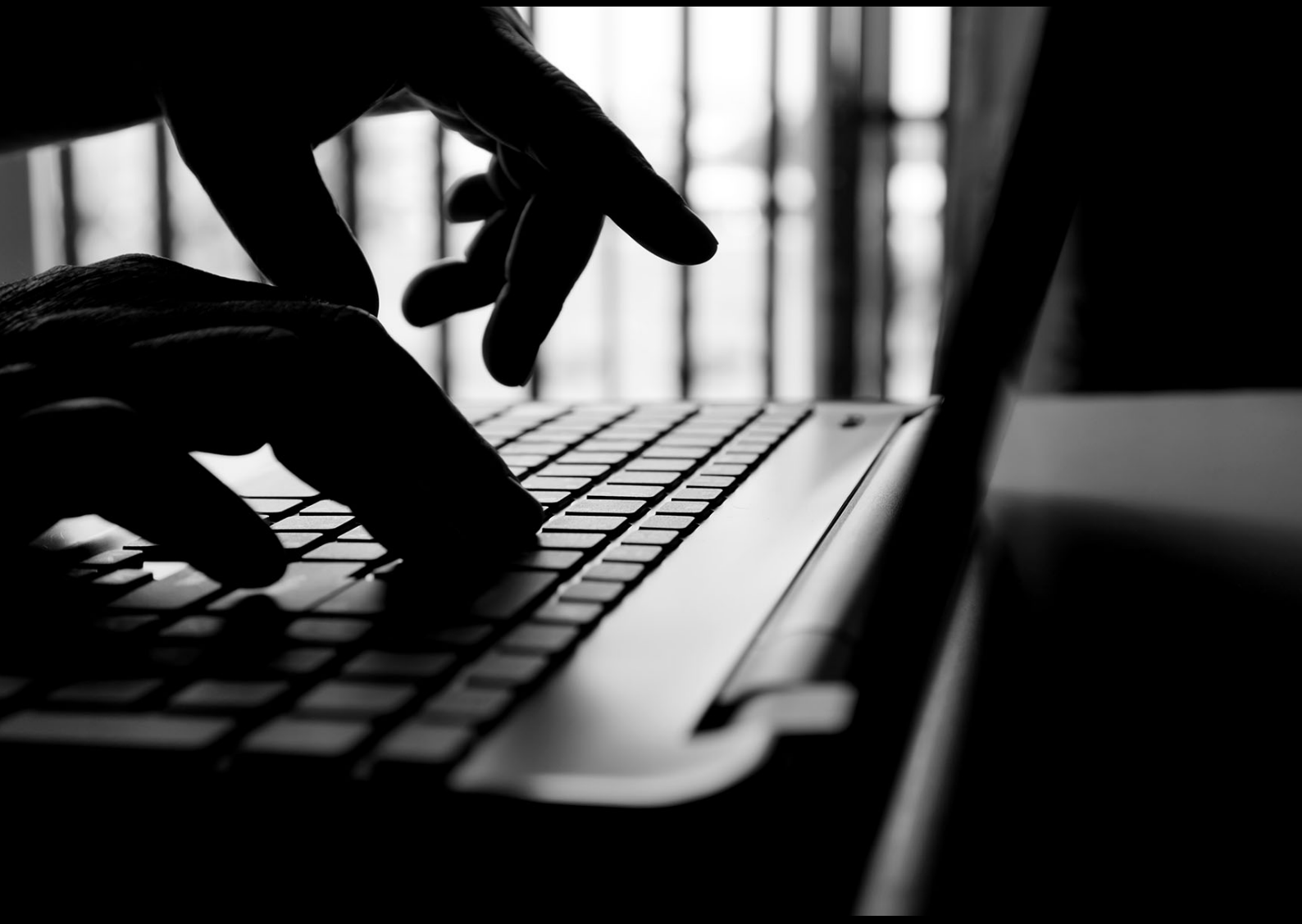
ACUMINOR REPORT

BEC FRAUD: A GOING CONCERN FOR CRIMINALS, AND A GROWING ONE FOR BUSINESS



ACUMINOR

"BEC FRAUD IS CONSIDERED ONE OF THE MAJOR CRIME THREATS FACING LAW ENFORCEMENT IN THE AMERICAS AND THE CARIBBEAN, AFRICA, ASIA AND THE PACIFIC -AND THE ILLEGAL PROFITS ARE NOT ABATING."

International Fraud Awareness Week seeks to promote anti-fraud education, detection and prevention. Following closely on the heels of European Cyber Security Month[1], the two awareness campaigns make convenient – and perhaps inseparable – bedfellows. As was recently highlighted by Interpol, cyber-enabled fraud has escalated in nearly every region worldwide, and is perceived by law enforcement to represent either a 'high' or 'very high' crime threat.[2] This Fraud Week thus presents an opportune moment to reflect upon financial crime in the digital era, and cast the spotlight on a particularly pernicious trend that has continued to flourish in 2022: business email compromise fraud. The discussion below examines, in brief compass, how the threat has evolved; the regulatory response; and, critically, how it may be detected by financial institutions seeking to stem the tide of illicit flows.

PERNICIOUS, PERSISTENT AND PROFITABLE

In 2019, business email compromise (BEC) fraud[3] was recognised as being among the fastest-growing cyber-enabled crime threats on a global scale, exposing the financial sector worldwide to billions of dollars in losses.[4]

In 2022, that threat has not dissipated. As was reported by Interpol last month[5], BEC fraud is considered one of the major crime threats facing law enforcement in the Americas and the Caribbean, Africa, Asia and the Pacific – and the illegal profits are not abating. US authorities reported in March that BEC fraud was the number one reported domestic scam in terms of money loss, amounting to nearly USD 2.4 billion last year.[6] Australian authorities have echoed that concern, reporting in August that BEC fraud is now "the most financially impactful kind of cybercrime".[7] Closer to home, Sweden's financial intelligence unit has confirmed that BEC scams feature heavily in fraud reporting[8], while the latest figures arising out of the UK quantify BEC losses as falling just shy of £8 million in the first half of this year.[9] With such significant revenues being generated, BEC attacks represent a profitable business model for the organised crime groups behind them – a going concern for fraudsters, and a growing one for business.

"LIKE OTHER ONLINE AND EXTORTION SCAMS, BEC FRAUD RELIES ON SOCIAL ENGINEERING, PROFITING FROM THE AVAILABILITY OF POTENTIAL VICTIMS' PERSONAL DATA."

TYPICAL BEC SCHEMES

BEC fraud is a species of authorised push payment (APP) fraud, involving the malicious redirection of funds. At the root of any APP scam – a category which includes, among others, romance, investment and invoice fraud[10] – is a deception that induces the victim to transfer funds into an account controlled by a criminal.[11] While methodologies vary, and continue to evolve, BEC fraud targets businesses through the use of either compromised or spoofed email accounts. Prominent schemes involve the use of email to masquerade as company leadership (commonly described as 'CEO fraud'); vendors ('supplier invoice fraud'); and professional services providers such as real estate agencies[12], lawyers or escrow firms. Hacked or spoofed accounts are typically used to contact internal staff, customers or the company's financial institution directly[13], instructing that funds be transferred (for purportedly legitimate business purposes) to criminal-controlled accounts.[14]

Like other online and extortion scams, BEC fraud relies on social engineering, profiting from the availability of potential victims' personal data. Fraudsters leverage information generated from phishing campaigns (another critical threat in 2022[15], as highlighted by our CISO earlier this month), or they purchase it via the Darknet. As Europol has observed, "the black market for compromised information is booming".[16]

A BEC attack may itself even be aimed at obtaining sensitive information for the purposes of another fraud or cyberattack in future.[17] Attacks are well-orchestrated, with fraudsters circumventing cybersecurity protocols, conducting reconnaissance and monitoring email traffic to determine the most lucrative point at which to strike. These enhanced measures increase both the prospects of success as well as the proceeds.[18]

"BEC ATTACKS ARE UBIQUITOUS, AND THE SOPHISTICATION OF SUCH SCHEMES CANNOT BE UNDERESTIMATED - PARTICULARLY IN THE LAST FEW YEARS."

MODERNISING THE MODI – AND THE MITIGATION

BEC fraud is not new on the fraud horizon, having first been detected in Europe a decade ago. At that time, it was predominantly committed in French language by organised crime groups operating from outside the EU.[19] Now, however, attacks are ubiquitous, and the sophistication of such schemes cannot be underestimated – particularly in the last few years.[20] The COVID-19 pandemic had a catalytic effect on the digitalisation of the workplace, and cybercriminals have adapted their *modi operandi* accordingly. This is unsurprising, given the tendency of criminal actors to become early adopters of new technologies.[21] For example, the FBI has recently observed the emergence of novel BEC schemes conducted via virtual meeting platforms utilising 'deepfake' audio.[22] In such schemes, compromised senior-level email accounts have been used to send virtual meeting requests to employees. Once in the meeting, a still picture of the 'hacked' executive has been used together with a 'deepfake' voice recording, claiming that the audio-visual function is not working properly. Employees have then been instructed to initiate funds transfers – a tactic which may be complemented with subsequent written instructions sent via the compromised email account.[23] While the general public remains relatively uninformed about the dangers of deepfake technology, organisations are beginning to view it as an even greater risk than identity theft.[24] Burgeoning crime-as-a-service business models deliver increased access to such tools, which is anticipated to drive further automation of cyber-enabled crime.[25]

Of course, criminals are not the only ones seeking to modernise: significant efforts are being made across the banking industry to respond to the rising tide of BEC and other APP scams. The increasing adoption of infrastructure such as 'Confirmation of Payee'[26] (CoP) is testament to that growing sense of urgency. CoP has been introduced across firms in the UK, France and the Netherlands, and is soon to expand to the Nordics as well (with the Nordic Payments Council due to publish its first rulebook on the CoP scheme by the end of this month[27]). Regulatory focus on APP fraud is particularly pronounced in the UK[28] – in addition to the CoP rollout[29], the regulator is agitating for a mandatory reimbursement scheme, whereby the banking sector would bear the cost of reimbursement for APP scam victims. This, it is hoped, will provide the requisite financial incentive for firms to devote further resources to fraud prevention.[30] Unfortunately, while the benefits of such initiatives are obvious, none are a silver bullet. The cost of reimbursement schemes is ultimately borne by consumers at large (while criminals continue to reap the benefits)[31] – and fraudsters appear to have already found a way to circumvent the CoP checking process via the use of money mules[32] (discussed further below).

THE BANKER'S DILEMMA

The difficulty for financial institutions in preventing BEC and other APP fraud lies in the fact that it is the victim themselves who has authorised the payment. This poses significant challenges for detection efforts – a point that has been made by the European Payments Council[33], and a predicament that has been the subject of recent judicial discussion in the UK. The last two years have seen a cluster of cases raising questions as to how a bank is expected to recognise, and respond to, risk indicators of APP fraud[34] – perhaps the most significant of which was decided by the UK's Court of Appeal in March .

The victim of a 'safe account' scam (another species of APP fraud) took her case to the High Court, arguing that the bank should have recognised the hallmarks of fraud and, accordingly, should have made inquiries prior to processing the transactions.[35] The customer was a music teacher, and her husband a retired medical physician. Both were deceived through an elaborate vishing operation (another trend explained by our CISO earlier this month), and believed their investments needed to be moved to a different account for safekeeping, to protect the funds from fraud. Acting on the instructions of the fraudster, the couple moved £950,000 – representing the bulk of their life savings – to a bank account held in the wife's name. In the days that followed, the couple attended different branches to instruct that payments of £400,000 and £300,000 be transferred to two separate company accounts held in the UAE. The deception was thorough: having been persuaded that anything they revealed to the bank would compromise a high-level police investigation, neither the customer nor her husband disclosed to branch staff that they were acting on the instructions of someone else.

Prior to the scam, transactions on the customer's account were consistent with her relatively modest income and living expenditure. It was thus argued on her behalf that the highly unusual deposit of £950,000 into her account, and the rapid subsequent transfers amounting to £700,000 to new international payees, ought to have been identified as suspicious transactions meriting closer interrogation.

The Court, however, disagreed. The case was dismissed on the basis that the argument advanced by the customer was commercially unrealistic, and that the bank could "not be expected to carry out such urgent detective work, or treated as a gatekeeper or guardian in relation to the commercial wisdom of the customer's decision".[36] The Court held that the 'red flags' pointed to by the customer were only discernible with the benefit of hindsight – and that it was unclear why they should be regarded as inherently suspicious in the first place.[37] On appeal, however, the Court of Appeal took a different view. While a bank's primary duty towards its customer is the prompt execution of payment instructions (and to exercise reasonable care and skill while doing so), there exists a separate duty, to refrain from executing an order if the circumstances would put an ordinary prudent banker on inquiry.[38]

This, naturally, begs the question as to when a banker will be on inquiry – what can an ordinary prudent banker be expected to recognise as indicators of risk? While the appeal decision was no doubt a welcome one for the victim, the original decision highlights nonetheless an important point. As articulated by the judge at first instance (and more bluntly stated now): people who work in banks are not there to be security guards. Staff processing payment instructions tend to be client-facing, tasked with a quasi-administrative, customer service function – and they aim to please the customer. It is that willingness to help, and reluctance to hinder, that is so readily exploited by the fraudster. Ameliorating the tension between the banker's competing duties is not an easy task, and demands heightened awareness and understanding of the risk indicators for BEC and other APP fraud.

"AVAILABLE INTELLIGENCE FIRMLY ESTABLISHES THE EXISTENCE OF MULTIPLE FACTORS WHICH MAY AROUSE SUSPICION THAT A TRANSACTION HAS BEEN PROCURED BY FRAUD."

RECOGNISING THE RISKS

Available intelligence firmly establishes the existence of multiple factors which may arouse suspicion that a transaction has been procured by fraud (and indeed, the 'red flags' pointed to by the customer in the case described above are archetypal examples[39]).

INTERNATIONAL TRANSACTIONS

Just as BEC attacks transcend borders, so, too, do the flows of illicit profits. Authorities in Sweden have, for example, identified that the proceeds of BEC fraud against Swedish companies are typically laundered internationally, whereas local money mules deal almost exclusively with the proceeds of foreign attacks. An overrepresentation of local mule accounts with links to Nigeria suggests that BEC networks active in that region are recruiting mules in Sweden.[40] Meanwhile, in the USA, authorities have reported that banks in Thailand and Hong Kong were the primary destinations for fraudulent BEC transfers in 2021, followed by China, Mexico and Singapore.[41] Outgoing transactions to new beneficiaries abroad, particularly those in jurisdictions identified as being higher risk, may thus warrant additional scrutiny.

MONEY MULES

Several risk indicators pertain to money mule activity, which is commonly seen in a variety of complex scams including BEC. The use of mule accounts is rising[42], possibly as a corollary of increasing APP fraud[43], and the systematic recruitment of money mules – or money mule 'herding' – has emerged as a clear trend in 2022.[44] Money mules serve as valuable intermediaries in the laundering chain, using both personal and business accounts to funnel illicit proceeds back to cybercriminals.[45] Deposits made into the accounts are often below the reporting threshold, and funds are typically withdrawn in a different geographic location, with little time elapsing between deposits and withdrawals.[46] Many mules are unaware that they are being used to channel money to criminal networks[47], having been recruited into such schemes under the false guise of employment, romantic relationships or investments.[48]

A recent case in the USA illustrates the point. Last month, an offender was sentenced to 25 years' imprisonment after being convicted of money laundering in relation to various online frauds including BEC. The offender had created multiple shell companies – none of which occupied physical premises, earned legitimate income or paid employee wages – and recruited at least eight money mules to open more than 50 bank accounts in the names of those businesses. The recruits were instructed to open multiple accounts at once, and to open additional accounts (at different banks) if any were closed for suspicious activity. They also opened personal bank accounts, often using false or stolen identities. The accounts were used to receive the proceeds from multiple BEC and romance scams – amounting to over USD 9.5 million – with funds quickly withdrawn following each deposit and circulated amongst the offender and his co-conspirators. [49]

"BEC AND OTHER FORMS OF APP FRAUD CAN BE EXPECTED TO BE THE SUBJECT OF ONGOING POLICE AND REGULATORY FOCUS AS WE MOVE INTO 2023. FINANCIAL INSTITUTIONS ARE WELL ADVISED TO ENSURE THEIR SYSTEMS APPREHEND AND RESPOND TO THOSE THREATS."

VIRTUAL CURRENCY

Another emerging trend identified by the FBI involves the abuse of virtual currency. There has been an increase in schemes where BEC criminals either: [50]

- Arrange for the target of a BEC attack to transfer funds to a cryptocurrency exchange directly; or
- Arrange for the payment to be made to an account established using a stolen identity, following which the funds are then exchanged into virtual assets.

Cryptocurrency was not identified as a feature of BEC fraud until 2018; however, in light of increasing reports, the FBI anticipates that the trend will continue to grow in the coming years.[51]

CONCLUSION

Undoubtedly, in the two decades since Fraud Week began, the financial services sector has taken considerable strides in embracing its remit. It is, however, a quickly evolving horizon. Cyber and financial crimes are almost invariably linked[52], and threats such as BEC have developed in parallel with digital innovations. Indeed, each incarnation of APP fraud merits its own dedicated discussion – a task which is regrettably beyond the scope of this paper, but which is ultimately essential in ascertaining relevant indicators of potential risk. Certainly, BEC and other forms of APP fraud can be expected to be the subject of ongoing police and regulatory focus as we move into 2023. Financial institutions are well advised to ensure their systems apprehend and respond to those threats.

1 And its various iterations around the world, observed annually in October.

2 INTERPOL. (2022, October 19). Financial and cybercrimes top global police concerns, says new INTERPOL report [Press release]; and INTERPOL. (2022). 2022 Interpol Global Crime Trend Summary Report. According to the accompanying press release dated 19 October 2022, the full report is restricted to law enforcement.

3 BEC fraud is also commonly referred to as email account compromise (EAC) fraud. It is also variously described as 'business email fraud', 'business email scams' or simply 'email fraud' – however, as has been observed by Interpol, those descriptors "do not address the e-mail compromise that enables the fraud": see INTERPOL. (2021). ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook from the ASEAN Cybercrime Operations Desk.

4 See, e.g., Egmont Group. (2019, July 30). Bulletin on Business Email Compromise Fraud; Justice Committee. (2022, October 18). Fraud and the Justice System (Fourth Report of Session 2022-23). House of Commons; and INTERPOL. (2019, October 9). INTERPOL urges public to #BECareful of BEC fraud [Press release].

5 INTERPOL, supra n 2.

6 FBI Internet Crime Complaint Centre (IC3). (2022, March). 2021 Internet Crime Report.

7 Department of Home Affairs. (2022, August 23). Cyber Security Industry Advisory Committee Annual Report 2022. See also Australian Federal Police. (2021, July 10). Business Email Compromise cost Australian victims more than $79 million in the past year [Press release].

8 Finanspolisen. (2022, January 26). Bedrägeri och pennningtvätt: Analys av bedrägerier ur ett brottsvinstperspektiv. Polismyndigheten.

9 UK Finance. (2022). 2022 Half Year Fraud Update.

10 UK Finance, the leading industry body for financial services in the UK, identifies eight types of APP fraud: Purchase scam; Investment scam; Romance scam; Advance fee scam; Invoice scam; CEO fraud; Impersonation (Police/Bank staff); and Impersonation (Other): see UK Finance. (2022). 2022 Half Year Fraud Update.

11 See, e.g., European Payments Council. (2021, November 24). 2021 Payment Threats and Fraud Trends Report; and Brown, J. & Shalchi, A. (2021, February 23). Banking Fraud (Briefing Paper no. 8545). House of Commons Library.

12 In the USA, for example, the Secret Service has warned of a sharp rise in BEC incidents specific to the real estate sector – a trend also observed by the FBI, in addition to a rise in BEC schemes targeting the entertainment and commercial food sectors: U.S. Department of the Treasury. (2022, March 1). National Money Laundering Risk Assessment.

13 Note though that such transfers do not fall within the APP category, as they constitute an unauthorised payment. The distinction arises given that it was a fraudster, rather than the corporate customer's legitimate representative/agent, who gave the payment instructions to the financial institution.

14 See, e.g., Egmont Group, supra n 4; and INTERPOL. (2021). ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook from the ASEAN Cybercrime Operations Desk.

15 INTERPOL, supra n 2.

16 Europol. (2021). Internet Organised Crime Threat Assessment 2021. Publications Office of the European Union, Luxembourg.

17 Egmont Group, supra n 4.

18 Australian Cyber Security Centre. (2021). ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021.

19 Europol. (2019, July 22). Focus on CEO Fraud [Press release].

20 See, e.g., Europol, supra n 16.

21 Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab. Publications Office of the European Union, Luxembourg.

22 FBI IC3. (2022, February 16). Business Email Compromise: Virtual Meeting Platforms [Public Service Announcement]. As described by Europol, 'deepfake' technology uses artificial intelligence to produce audio-visual content that convincingly depicts people saying or doing things they never did, or fabricating entirely new personas: see Europol, supra n 21.

23 See also FBI IC3, supra n 6.

24 Europol, supra n 21.

25 Ibid.

26 The CoP service is designed to mitigate APP fraud by allowing the payer to enter the account name for the intended beneficiary, which is then verified against the name held on file by the recipient bank. If there is no match, the payer is informed, and can reconsider whether they wish to make the payment: see, e.g., European Payments Council, supra n 11

27 European Payments Council. (2022, October 26). The Nordic Payments Council: harmonising payments in the Nordics [Press Release]. See also Nordic Payments Council. (2022, September). Public consultation – Confirmation of Payee Scheme 2022.

28 See Payment Systems Regulator. (2022). Annual plan and budget 2022/23; Financial Conduct Authority. (2022, April 7). Our Strategy 2022 to 2025; and Financial Conduct Authority. (2022, April 7). Business Plan 2022/23.

29 Payment Systems Regulator. (2022, October 11). PSR directs 400 firms to introduce the payment protection measure, Confirmation of Payee [Press Release].

30 See Payment Systems Regulator. (2022, September 29). CP22/4: Authorised push payment (APP) scams: Requiring reimbursement.

31 See Justice Committee, supra n 4.

32 UK Finance. (2021, February 4). APP fraud – less talking, more acting [Blog].

33 European Payments Council, supra n 11.

34 See, e.g., Sekers Fabrics Ltd v Clydesdale Bank Plc [2021] CSOH 89 (26 August 2021); Tecnimont Arabia Ltd v National Westminster Bank Plc [2022] EWHC 1172 (Comm) (17 May 2022); and Philipp v Barclays Bank UK Plc [2021] EWHC 10 (Comm) (18 January 2021), which was successfully appealed in Philipp v Barclays Bank UK Plc [2022] EWCA Civ 318 (14 March 2022).

35 Note that the UK regulator has since proposed the introduction of a mandatory reimbursement scheme: see Payment Systems Regulator, supra n 30.

36 Philipp v Barclays Bank UK Plc [2021] EWHC 10 (Comm) (18 January 2021) at [172].

37 Ibid at [171].

38 Philipp v Barclays Bank UK Plc [2022] EWCA Civ 318 (14 March 2022) at [27]. Whether or not the duty arose in the particular circumstances of the case, however, was a separate question which could only be answered at trial.

39 Of course, in that case, whether a bank could have been expected to recognise the significance of such indicators in March 2018 (i.e. when the fraudulent transactions occurred) is a separate question which can only be determined by the Court at trial.

40 Finanspolisen, supra n 8.

41 FBI IC3. (2022, May 4). Business Email Compromise: The $43 Billion Scam [Public Service Announcement].

42 INTERPOL. (2022, August 10). #YourAccountYourCrime: Global campaign exposes use of money mules [Press Release].

43 Cifas. (2022, April 28). Fraudscape 2022.

44 INTERPOL. (2022, June 15). Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams [Press Release].

45 INTERPOL, supra n 42.

46 See Egmont Group, supra n 4; Cifas, supra n 43; and U.S. Department of the Treasury, supra n 12.

47 Egmont Group, supra n 4.

48 INTERPOL, supra n 42.

49 U.S. Attorney's Office, Northern District of Georgia. (2022, October 3). Georgia man who laundered millions from romance scams, Business Email Compromises, and other online fraud receives 25-year sentence [Press release].

50 FBI IC3, supra n 41. See also U.S. Department of the Treasury, supra n 12.

51 FBI IC3, supra n 41.

52 INTERPOL, supra n 2.

ACUMINOR

A BRIGHTER WORLD

Terms of use
You are free to use this report for your own personal development, in internal training or in other risk management activities. You are of course not allowed to resell this report, nor claim that you have made it yourself.

Please remember to state the source as follows:

Acuminor Report - BEC Fraud: A going concern for criminals, and a growing one for business

Sveavägen 140
113 50 Stockholm
SWEDEN

1 Poultry
London EC2R 8EJ
UNITED KINGDOM

acuminor.com
+46 8 121 586 30
relations@acuminor.com

© Acuminor 2022