BUSINESS EMAIL COMPROMISE FROM THE CRIMINAL LAW PERSPECTIVE

Maxim DOBRINOIU[*]
Nicoleta GRATII[**]

Abstract

With nearly 85% of worldwide organizations being hit at least once, the Phishing attack has become one of the most significant cybercrime vectors that affect the business environment annually, with great loss in terms of money, assets, financial and personal data, confidential information and intellectual property rights. Hackers evolved both in sophistication and persistence of the methods they use in performing these attacks, while 97% of the users are still unable to roughly or properly recognize a simple phishing email. Amongst different types of Phishing, the Business Email Compromise variant represents one of the most employed tool by attackers for hacking human minds, and manipulate victims into performing various actions that eventually cause them loss. Most of the national legislations already have legal provisions to cope with this kind of menace, but the trend is to treat such scam as cyber-related offence or crime, based on the simple reason that it is performed by information technology means. While the judicial practice in this scenario is often ripped off by different interpretations of the existing legal provisions available, this material tries to come up with the most suitable criminal indictment solutions for this fraud, highlighting both technical and legal aspects that may help judges, prosecutors, lawyers, law enforcement agents and other legal practitioners in properly solving their cases.

Keywords: *business email compromise, fraud, scam, phishing, social engineering, criminal law, cybercrime, IT law, CEO fraud*

1. The concept of Phishing

Phishing has risen as a unique threat in the cyber environment, a menace that succeeds to bind together technology, psychology, sociology and communication skills, in exploiting the weakest link of the human defense and personal security: the mind.

Acting as a Social Engineering (SE) attack, Phishing is far more dangerous when directed to target a specific destination (individual, business, organization) – thus known as Spear Phishing.

Phishing itself is not intended to harm a computer system or data, as it hasn"t a malicious payload. Instead, it lures the victim to access its dangerous hyper-connections (known as "links") inserted in "to-good-to-be-true" email messages. Technically, the links are crafted to drive the user"s browsers to certain web pages (usually fake or in control of the offender). The human exploit is then realized as soon as the user is deceived and agrees to perform the offender"s will.

The COVID-19 pandemic offered a good opportunity to different bad actors (scammers, fraudsters, hackers) to target individuals and businesses alike, especially in the "work-from-home" scenarios.

Statistics of 2020[1] show that nearly 85% of the businesses have been hit by Phishing, while 97% of the Internet users do not have the capacity to recognize such an attack. On a regular basis, 30% of Phishing emails are opened by the users, and 12% of them further click on the links provided in the messages. Every month, 1.5 million new Phishing websites are created and used by fraudsters.

One particular thing is of a special attention: 96% of all targeted attacks are intended for intelligence-gathering[2]. Intelligence that is further used by the offenders in a reconnaissance activity with the intent to target a particular individual or business with the final aim to cause them loss of money or property. Such derived attack often comes as a scam, a swindle or a fraud, and it is known as Business Email Compromise (BEC).

According to government agencies[3], Business Email Compromise or Email Account Compromise (EAC) poses as a sophisticated scam targeting both large/medium/small businesses and sometimes individuals, frequently carried-out by an intruder breaking-in and taking-over an email account or just by spoofing an email address in order to determine an individual target to undertake financial transactions or transfers to bogus bank account or wire recipients.

While back in 2013, BEC scam was performed by simply creating a "just-like-the-original" fake email address (account) or by spoofing a genuine email address mostly belonging to a high rank official with a financial organization, a company or an organization (ex. CEO, CFO etc.), with the request of wire money transfer to be made to fraudulent locations, this kind of fraud evolved in the years after, both in technicity and

[*] Associate Professor, PhD, Faculty of Law, "Nicolae Titulescu" University, Bucharest (e-mail: maxim.dobrinoiu@univnt.ro).
[**] Master student in Criminal Sciences, Faculty of Law, "Nicolae Titulescu" University, Bucharest (e-mail: nicoletam39588@univnt.ro).
[1] https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/.
[2] Ibidem.
[3] https://www.fbi.gov/contact-us/field-offices/anchorage/news/press-releases/fbi-releases-2020-internet-crime-report.

sophistication, posing a far greater danger to businesses that regularly conduct electronic (wire) banking transactions, money transfer and payments.

In its 2020 IC3 Report[4], the FBI warns about a new trend in BEC/EAC scams, where has been observed an increase of using Identity Theft at a larger scale and (illegally obtained) funds being converted into cryptocurrencies.

Holding the 9th position in the 2020 top US Cyber Crime by Type, BEC/EAC has reached the Number 1 position in terms of financial loss, with a figure of nearly 1.9 billion USD (with 1.7 billion USD in 2019), a strong indicator of the criminal potential these scams reached to.

The industry alike, especially financial companies see BEC and EAC as a damaging form of cybercrime, capable of producing loss worth billions of USD a year, especially during the COVID-19 pandemic, when two factors contributed the most in escalation of the scams: new work-from-home business model and the increasing number of new foreign clients/suppliers/partners etc.

The experts warn that no industry is risk-free against BEC/EAC. In 2020, 93% of these attacks hit energy and infrastructure sector, while the overall rise reached 75% of the tracked business[5].

Banking sector has its own big concern about BEC/EAC, as recent statistics[6] show that 86% of the bank employees and representatives think that business email compromise and account takeover fraud are the greatest risks to their business. In response to that menace, 37% of the bank respondents intend to invest significantly in check fraud technology in the next 12 months.

At this level of industry, BEC/EAC are often perceived as "cyberattacks designed to gain access to critical business information or to extract money through email-based frauds", where the emails are just an attempt to convince an employee to reveal "critical business or financial information or process a payment request" that would never be done otherwise[7].

For all that, the companies admit that BEC/EAC may be something more complex than a simple email spoofing, especially when they are confronted with sophisticated "account takeover" attacks – with the attacker using intrusion tactics, techniques and procedures (TTP), such as (Spear) Phishing and Reconnaissance. While inside an email account, the attacker may find very useful information, like personal data of the victim"s contacts (vectors for new BEC/EAC attacks), calendar events, as well as the content of the electronic correspondence which is of a great importance when the attacker need to study the victim"s profile (as an employee or a boss), especially the payment habits or financial recurrences (both business and personal).

The success of an BEC/EAC attack rely on both technical aspects and human (victim) behavior.

According to cyber-security specialists at CSO Online[8] the technical flaws in confronting BEC/EAC may include:

- Desktop email client and web interface (e.g. Gmail, Yahoo) not synchronized and run the same version;
- Not establishing multi-factor authentication (MFA) for business email accounts;
- Not forbidding "automatic forwarding" of emails to external addresses;
- Not properly monitoring email Exchange servers for changes;
- Not often reviewing the use of legacy email protocols (IMAP, POP3);
- Not logging the changes to mailbox login and settings for at least 90 days;
- Not enabling security features to block malicious emails.

While the human (mis)behavior consists of:

- Not being attentive (aware) of "last-minute" change of email address of domain name of the contacts the employee often exchanges messages with;
- Not checking the misspelling in email address (often, the attackers switch the letters like "O" or "I" with figures like "0" and "1", or just eliminate certain letters of figures);
- Not adding banners in inbox to messages received outside the organization;
- Not reporting suspicious payment requests;
- Not setting-up alerts for suspicious behavior in exchanging messages with other contacts.

Despite the use of (even highly) sophisticated tactics, techniques and procedures, BEC/EAC scams, usually known as CEO Frauds or Man-in-the Email scams, ultimately target individuals in a way that succeed to manipulate them and determine (or persuade) to perform different actions that otherwise they probably would have not done.

So, they appear to be more like social engineering (SE) type "confidence tricks", than real computer fraud, while in both scenarios the aim is the money, as more and more specialists tent to admit[9].

In such way, dealing mostly with human (brain) hacking, and not computer hacking, the legal system has fallen apart in identifying the most appropriate way to bring down to justice and press charges against the perpetrators.

But, what is really there, from the criminal law perspective?

[4] Issued on April 9, 2021.
[5] https://securityboulevard.com/2021/02/business-email-compromise-is-on-the-rise-again/.
[6] https://bankingjournal.aba.com/2021/02/survey-banks-see-business-email-compromise-as-biggest-threat/.
[7] https://news.microsoft.com/on-the-issues/2020/07/23/business-email-compromise-cybercrime-phishing/.
[8] https://www.csoonline.com/article/3600793/14-tips-to-prevent-business-email-compromise.html.
[9] https://eyfinancialservicesthoughtgallery.ie/ceo-fraud-an-ancient-attack-with-a-new-dimension/.

2. Doctrine views on scam/fraud

When it comes to law enforcement, it is of a great importance to define the terms, and rely on the most appropriate meaning in order to get the best from a variety of possible criminal charges.

Either is about Advance Fee Schemes or BEC/EAC, Business Fraud, Charity and Disaster Fraud, Credit Card Fraud, Elder Fraud, Identity Theft, Internet Fraud, Investment Fraud, Nigerian Letter (or "419 Scam") Fraud, Letter of Credit Fraud, Money Mules, Non-delivery of Merchandise, Ponzi Schemes, Pyramid Schemes, Romance Schemes or Sextortion, they all have one thing in common: human hacking (brain hacking) or human manipulation.

National criminal legislations usually drive on slippery slopes when about to differentiate among the above-mentioned illegal activities, and thus don"t make strong and clear difference between scam and fraud.

In the English-speaking countries" law, the term "fraud" is rather a concept, although not a crime in itself, it exists at the core of a variety of criminal statutes[10]. According to author Ellen S. Podgor, "one finds generic statutes, such as mail fraud or conspiracy to defraud being applied to an ever-increasing spectrum of fraudulent conduct", while "in contrast, other fraud statutes, such as computer fraud and bank fraud present limited applications that permit their use only with specific conduct".

Other English Law based authors[11] defined fraud as "an intentional or deliberate misrepresentation of the truth for the purpose of inducing another, in reliance on it, to part with a thing of value or to surrender a legal right". Fraud, then, appears to be "a deceit which, whether perpetrated by words, conduct or silence, is designed to cause another to act upon it to his or her legal injury".

"Fraud", as well as "fraudulent" are terms united by a common sense: deceit[12], and both has the meaning of a conduct with a purpose to deceive in order to get hold of something. That is why in some legislation (ex. UK) "fraud" is the short name for the crime of "fraud by false representation".

"Scam", however, has the meaning of a fraudulent business scheme, a stratagem for a gain or a swindle[13]. But in any case it involves human manipulation through deceiving.

Although there seems to be little or no difference between "fraud" and "scam", the general perception is that "scam" always involves money, whereas "fraud" may incur more other losses (apart from money).

Fraud is a term also used in the rest of the world criminal legislation, depicting various instances of criminal activity where deceit is often used to manipulate a person or to evade (bypass) state regulations for a personal gain.

More or less, the crimes having fraud as a drive, are usually gathered under the same title (or section) within the nations" criminal codes, such as "crimes against property".

3. Doctrine views on computer-fraud

Based on the legal provisions of the Council of Europe "Budapest" Cybercrime Convention of 2001[14], most of the European countries created, modified, or updated their own criminal laws including different crimes against confidentiality and integrity of data and computer systems, as well as the so-called "computer-related crimes" (computer-related forgery and computer-related fraud).

Article 8 of the CoE Convention on Cybercrime provides Member States with a model for criminalization of a behavior against the trust and the property by the means of computer data and computer systems, as follows:

"Computer-related fraud – Each member state shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- any input, alteration, deletion, or suppression of computer data,
- any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or another person".

Currently, the CoE Convention on Cybercrime has been ratified by 47 members of the Council of Europe and adopted by another 31 non-European countries, with most of its legal provisions being implemented into national criminal legislation on cybercrime.

And thus, having a rising trend in technology and with a new (or reshaped) criminal provision in place, a new form of fraud offence emerged – the computer-related fraud, usually with slightly harsh punishment with imprisonment (comparing to different other types of fraud or scams).

Analyzing the legal provision promoted in Article 8 by the CoE Convention on Cybercrime, one can notice that there is no mention of the "deceiving a person", "misleading" or "turning a person of doing something".

---

[10] Podgor Ellen S., *Criminal Fraud*, American University Law Review 48, no. 4 April 1999: 729-768.

[11] Edward J. Dewitt Et Al., *Federal Jury Practice and Instructions*, 16.8, 4th edition, 1992.

[12] „The act of misleading another through intentionally false statements or fraudulent actions" (according to https://legal-dictionary.thefreedictionary.com/deception).

[13] scam. (n.d.) *American Heritage® Dictionary of the English Language, Fifth Edition*. (2011). Retrieved April 10 2021 from https://www.thefreedictionary.com/scam.

[14] Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

It is all about interfering with (or acting upon) computer data and computer systems, with "fraudulent or dishonest intent" of (just) the perpetrator on its way to procuring an economic benefit, while causing a loss of a property (that includes other values, such as money) to a person (the victim).

In some criminal legislations (in Romania, for example), the computer-related fraud was long time considered as a special provision, thus being preferred by the law enforcement, prosecutors and judges to be used in pressing criminal charges against individuals suspected for the commission of various scams especially on the online markets, like eBay, Amazon and so.

Even the cases of BEC/EAC are usually being "solved" by referring to computer-related fraud as the best option for a criminal charge, merely due to an increased penalty and the scope for a better prevention against this kind of misconduct.

4. Business Email Compromise at the crossroads between traditional fraud and computer-fraud

As we have showed, BEC/EAC is a type of scam or fraud that implies different tactics, techniques and procedures, with the use of computer data and systems or other means of electronic communications.

But, apart from using computer systems and data (mostly email messages), BEC/EAC is more about the perpetrator taking advantage of multiple bad habits of the victims in using electronic means of communication, and the manipulation of their behavior in order to give up sensitive information (personal, confidential etc.) and, more important, to perform certain acts that eventually result in loss of money or property (for the benefit of the fraudster/scammer)[15].

Although it may look like the same, fraud and computer-related fraud are two individual offences with different approach from the national criminal legislations.

The common things that seem to bind them are:

- they both target property (in general) and money (in particular) of another (individual or organization)
- they both produce or intend to produce loss
- they both use tactics, techniques and procedures from the cyberspace (email, short messages, instant chat, computers, smartphones etc.)

The differences are somehow essential.

The first difference consists of who/what the perpetrator (fraudster) is acting upon:

a) in the case of a simple fraud (scam/swindle – for example BEC/EAC), the criminal actor uses deceit as his principal weapon against the victim. Deceit is successful if the offender and the victim don"t actually meet in person, but communicate via email (or other means). Deceit works especially when the factual data (the misrepresentation) presented by the offender contains enough "truth" that determine the consciousness of the victim to lay down the psychological barriers, to enter in a "comfort status" in the relationship with the ideas provided by offender and finally to get into the "trust status" thus accepting the offender data input as "worth to be followed". And, this is the moment when fraudster takes advantage of the victim"s "trust status" and further conduct manipulation against her.

b) in the case of a computer-related fraud, the offender creates, modifies, deletes or suppresses computer data, and even interferes with the functioning of a computer system in order to cause loss (of property or money), thus no relying on the victim"s behavior and not trying to manipulate her at all. The victim simply does not have any role in being defrauded or losing her property or money.

In the BEC/EAC scams, the funds are consciously authorized or handed-over to the offender by the victim herself, while in the computer-related fraud scenarios, the victim is not participating at all, and just finds out, discovers or is noticed about the result of the fraud/scam: loss of her property.

Such conclusions are also shared by other authors. In one opinion[16], computer data and computer systems are the target of the offender in the case of computer-related fraud, whereas in the case of simple fraud (scam/swindle), they are just means by which the offender is deceiving the victim.

In the simple fraud (scam, swindle), if the offender relies on false computer data (through input, alteration, deletion or suppression of data – resulting in non-authentic data with the aim to be considered to legal purposes) in order to create a misrepresentation of the truth and manipulate the victim, along with the crime of fraud, a computer-related forgery crime should also be considered as a valid criminal indictment.

Another perspective[17] that we embrace is that, in the legal relationship between the traditional fraud (scam, swindle) and the computer-related fraud, there is no possibility of a legal concurrence of offences. This is merely a conflict of legal provisions, that usually requests the legal practitioners to choose the one that is the most applicable for a given scenario.

5. Conclusions

For all that we have said and demonstrated in this paper, we came to the conclusion that in the case of traditional fraud, performed by the means of electronic

[15] See also Andrew Marshall Hardy, head of fraud risk for CCIB in article *The high cost of business email compromise fraud*, available at https://www.sc.com/en/feature/the-high-cost-of-business-email-compromise-bec-fraud/

[16] George Zlati, *Treatise on Cybercrime*, vol. I, Solomon Publishing, 2020, p. 454.

[17] Idem, p. 453.

communications or computer data (e.g. BEC/EAC scam, swindle), the following offences shall be considered (given the tactics, techniques and procedures, as well as the technology used):

- illegal access to a computer system (with regard to the email account of the victim, that the offender breaks-in)
- unauthorized transfer of computer data (if the offender gets data – personal, financial, confidential – out of the email account)
- computer-related forgery (if the offender interferes with computer data thus resulting unauthentic information to be used in deceiving the victim prior to manipulate her to surrender the property or money)
- traditional fraud (scam, swindle) by the means of electronic communications or computer data

all together in a legal concurrence of offences.

References

- George Zlati, *Treatise on Cybercrime*, vol. I, 2020, Solomon Publishing;
- https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/;
- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise;
- https://www.ic3.gov/Media/Y2020/PSA200406 ;
- https://www.proofpoint.com/us/resources/white-papers/bec-scams-2020-2019;
- https://news.microsoft.com/on-the-issues/2020/07/23/business-email-compromise-cybercrime-phishing/;
- https://www.cyber.gov.au/acsc/view-all-content/publications/protecting-against-business-email-compromise;
- https://www2.deloitte.com/us/en/pages/advisory/articles/five-ways-mitigate-risk-business-email-compromise.html;
- https://www.google.com/amp/s/www.csoonline.com/article/3600793/14-tips-to-prevent-business-email-compromise.amp.html;
- https://www.sc.com/en/feature/the-high-cost-of-business-email-compromise-bec-fraud/;
- https://www.secureworldexpo.com/industry-news/top-10-cybercrime-insurance-claims;
- https://gatefy.com/blog/real-famous-cases-bec-business-email-compromise/;
- https://eyfinancialservicesthoughtgallery.ie/ceo-fraud-an-ancient-attack-with-a-new-dimension/;
- https://securityboulevard.com/2021/02/business-email-compromise-is-on-the-rise-again/;
- https://bankingjournal.aba.com/2021/02/survey-banks-see-business-email-compromise-as-biggest-threat;
- https://www.sc.com/en/feature/the-high-cost-of-business-email-compromise-bec-fraud/.