Carnival of Cybercrimes - Taking off the Mask of Synthetic Identity Theft

Larisa-Mădălina MUNTEANU
Data Protection Lawyer and Deputy Data Protection Officer, JS Information Governance Ltd, Peterborough, the United Kingdom
larisa@js-ig.com

Abstract

This article portrays a comparative and doctrinal analysis that aims to combine theoretical and applicable knowledge over a deeply rooted, yet still unfamiliar cybercrime: synthetic identity theft. The jurisdictional dimensions explore the European Union (EU), United Kingdom (UK) and United States (US) in terms of expertise, legal initiatives, regulations and practical cases. As a prerequisite, the study has addressed the connection with identity theft and identity fraud as the Criminal Law "labels" it generally belongs to. Moreover, the most thought-provoking part represents analysing the nexus between synthetic identity theft and personal data protection, focused on security incidents. On this latter point, personal data breaches are proven as frequently being both a cause and an effect for synthetic identity theft. Subsequently, this turns out to have significant impact on individuals and organisations alike, predominantly in the financial sector, although harm may take several shapes.

Index terms: cyberattacks, financial fraud, personal data, regulatory framework, synthetic identity theft

1. Introduction

In modern times, digitalisation has become the foundation of our daily activities, impacting on all sectors – health, communications, education, economy, justice etc. However, life has taught us there is always "the flip side" of the coin. So, what is the less advantageous part of this evolutionary road? It could be our exacerbated dependence on technology, the psychological side-effects, or perhaps the privacy risks we expose to, although inadvertently. With respect to the latter, by far, one of the most impactful ones refers to cybercrimes, concomitantly and proportionally escalating as new technologies emerge. For example, the COVID-19 pandemic has resulted in a notable increase in online transactions and processing of health data, which is considered a special category of personal data, according to the European Union and the United Kingdom's General Data Protection Regulation [1, Art. 9], [2, Art. 9]. This means cyberattackers have now reconsidered the focus of their activities – there may have even been cases where such data became more valuable than financial data. Thus, different social and technological changes have shaped the cyberspace and subsequently, the interests of the online-focused perpetrators. To confirm this, the Police Executive Research Forum has previously accentuated this advancement stating "as technology becomes more sophisticated, so have computer crime schemes" [3].

Furthermore, by overlapping the increase in financial fraud and impersonation, we can visualise synthetic identity theft. It is not a notion that emerged because of the pandemic, but has definitely flourished throughout this period. As interesting, yet challenging this cybercrime may be, this article

will explore synthetic identity theft in the following dimensions: theoretical and practical aspects, regulatory standpoint and privacy impact.

2. Conceptualisation

2.1. Theoretical aspects

ENISA [4] highlighted in the last report on cyber threats that identity theft has been increasing in frequency, mostly because of the convenience and accessibility brought by dark web and related forums to perpetrators interested in personal data. Bracker et al. [5] confirmed this increase, especially in the context of fraudulent activity during the COVID-19 pandemic. Moreover, identity fraud, concept used alternatively with identity theft and the act of impersonation, is one of the cybercrimes with significant impact on personal data: not only that it results in unlawful advantages, but it also leads to data breaches [6], which are detailed in Section 4.

At the same time, the context in which identity theft is identified, be it physical or digital, follows identical rules and steps, and thus, Bandler and Merzon [7] concluded that identity theft is usually "the gateway to cyber schemes". To continue, synthetic identity theft was considered this year "the fastest-growing type of identity theft" [8]. To confirm, ENISA's report from 2022 [4] listed the most frequent forms of identity theft as being credit card fraud and synthetic identity theft. At the same time, other studies have indicated a tight connection between these last two – synthetic identity fraud may additionally be used "to apply for credit cards or loans, as well as to bolster and improve additional fake customers' creditworthiness" [9]. Although that is the most usual hypothesis, the list of motives is open. For example, the founder of a US company providing security and privacy support to healthcare organisations emphasised the importance of medical data in this context and how the healthcare system can become a target of these cybercrimes too, in addition to the banking one [10].

Nowadays, the Federal Reserve has officially defined this phenomenon as "the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain". On these grounds, synthetic identity theft has crossed the borders of financial crimes and extended the scope towards a plethora of crimes [11]. Nonetheless, synthetic identities do not rely upon such consistent trails as real identities, and will most likely fail substantial verifications, leading to a resourceful approach that can be used for determining the authenticity of a person to the highest degree – "by evaluating the depth and consistency of information available about applicants in third party data systems" [12].

A study from the early 2000s transpired this phenomenon in a simple definition. The first important mention is that the author includes synthetic identity theft as part of account fraud, taking two possible routes: purely fabricated information or pairing real social security numbers with fictious names [13, p. 101]. Thus, this would result in unusual conclusion – identity theft can occur without stealing anyone's identity, in this case!? In reality, this may be the explanation as for why some studies refer solely to the second form mentioned above. However, it is clear that this differentiates synthetic identity theft from impersonation.

All in all, regardless of the specific definition, synthetic identity theft lies on an elaborated strategic foundation, due to the necessity to "slowly and methodically create an artificial, or synthetic person", context in which it becomes worrying that only a few people apprehend this threat [14]. This inherent complexity has led the Federal Reserve Systems of the United States to reach the drastic conclusion that "no single organization can stop synthetic identity fraud on its own" [15]. Furthermore, this conclusion was also stated in [12], accentuating "there has been no efficient way of uncovering synthetic ID fraud", yet such applications are generally not accepted due to the impossibility to match the name with the records of financial institutions.

2.2. Practical impact

Nonetheless, the practicalities of cybercrimes that are identity-related become of interest to modern researchers because the perpetrators have, nowadays, the convenience and assistance of dark web for obtaining digital goods [6]. However, it is interesting to notice that some authors concluded that a significant part of the unlawfully collected personal data shared on dark web "is never used for anything at all" [16, p.54].

On the other hand, in terms of side effects and potential harm, the United Nations Office on Drugs and Crime has pointed out in 2011 that the simple fact that an existing person is not in reality affected by synthetic identity theft should not be understood as being a harmless incident, referencing several studies that confirm that more than half of identity theft offences rely upon synthetic identities [17]. To continue, the negative effects are mostly quantified as delaying their detection and investigation, along with creating difficulties for the victims throughout the process. To support this perspective, the potential judicial side effects are recognised by older studies as well, referring to the debt collectors that may simply track the social security number back to the real person owning it, causing "reputational harm and emotional distress, in addition to wasting the victim's time and resources" [13, p.103]. A more recent study has highlighted that such identity theft should not be concerning as the only side effect to be identified is that it "drains wealth from the broader economy" [16, pp. 30-31].

One of the major cases involving synthetic identities happened in the US, when over $3 million was fraudulently obtained by two men. They commenced this scheme in 2017 and in 2020, they additionally took advantage of the Paycheck Protection Programme, as per the Coronavirus Aid, Relief, and Economic Security Act [18], aimed to support small businesses throughout the COVID-19 period. By using the stolen identities and creating synthetic ones, financial support was initially sent to the latter and subsequently, to the perpetrators' accounts [19]. This case echoes the 2022 report of the Pandemic Response Accountability Committee, explaining how the United States decided to include more security measures for identification purposes, such as a Personal Protection Identification Number (IP PIN), in addition to SSNs, enforcing "dual factor identity validation" [20, p.11]. However, way earlier than that, in 2006, a similar case proved the emergence of synthetic identity theft in the United States, after two men paired Social Security Numbers from credit reports with fictious identities and charged $760,000 to the synthetic "persons" created [21].

Thus, the Federal Reserve has prepared the Synthetic Identity Fraud Mitigation Toolkit early last year [22], with the aim to educate people and raise awareness in order to counter the maturing of this cybercrime, pinpointing even less discussed scenarios, such as using social security numbers of children, impeding later employment or loans [23].

3. Legal initiatives

From a legal perspective, the only binding international instrument on cybercrimes is the Budapest Convention on Cybercrime [24]. However, given the open clauses of the convention, it can be considered to have limited powers, planning to create a framework for the Signatories to follow in order to create harmonised and deeply rooted legal provisions. Among the categories of cybercrimes that are addressed therein, Article 8 is of interest for this study, urging the states to adopt legislation against computer-related fraud committed for obtaining economic benefits.

To continue, EU Member States have incriminated identity theft, but with no explicit reference to the synthetic form. As an example, "identity-related crime concerns in France mainly focus on document and financial fraud", leading to the initiative to introduce "an eID card with biometrics identifiers and based on centralised databases" [25, p.18]. However, this initiative was equally confirmed at EU level and the Member States were finally in the position to be bound by a Regulation urging them to shift to secure electronic ID cards by latest 2031, as a countermeasure to identity fraud,

along with ensuring national laws sanction such schemes [26, Recital 8, Art. 5]. Comparatively, Estonian citizens were using eIDs since 2002, based on a chip and two PIN numbers – serving as authentication and digital signature. Among others, the ID would allow the person to vote and purchase transport tickets too. By doing so, it was regarded as "resilient to cloning" and it meant identity theft could occur only if the card was stolen together with the PIN codes [25, p.23].

On the other hand, in the United Kingdom, the Fraud Act 2006 and Digital Fraud Committee highlighted in their last report the importance of identity theft in the ecosystem of fraud, especially given the criminal activity of enterprises on dark web that sometimes create synthetic identities, "yet it remains out of scope of criminal offences" [27, para. 458]. As a response, the Government considered existing legislation already covers this type of fraud by applying the Fraud Act 2006 [28] and the Computer Misuse Act 1990 [29]. On top of that, it should be added that the Identity Documents Act 2010 incriminates the possession of false identity documents under certain conditions [30, s. 4-6], where "false" is defined as encompassing inaccurate or omitted information "in a tendency to mislead" [30, s.9(4)a)]. In my opinion, synthetic identity theft can be covered by this definition, if we accept that the false information added to the authentic personal information lead to an "inaccurate" identity. However, the Committee emphasised the necessity to regulate identity theft as "a specific criminal offence" and alternatively, "a serious aggravating factor in cases of fraud" [29, para. 459]. Perhaps, this is the reason why some authors considered "the UK scheme of identity crime statutes is not well thought out", representing a "hodgepodge of different statutes" [31].

Nevertheless, the United Kingdom Government has adopted a process for organisations to follow when checking individuals' identities [32]. As a result, this guidance explains the impact of disregarding synthetic identities and identity fraud and labels the confidence levels upon such verifications as low, medium, high and very high. Of interest to this article is the first category, where synthetic identities are included.

Comparatively, in the US, incriminating identity theft took a more straightforward route, by having it listed in the United States Code (U.S.C.), in Title 18 - Crimes and Criminal Procedure, section 1028, called "Fraud and related activity in connection with identification documents, authentication features, and information" [33]. However, the Identity Theft and Assumption Deterrence Act of 1998 was the first legal instrument to officially describe and prohibit identity theft as a federal crime, substantiating criminal laws [34]. It is essential to note that this prohibition extends to the "intent to commit, aid or abet" such unlawful acts constituting violations of federal law or felonies under statal or local law. With respect to aiders and abettors, the U.S.C. has addressed the social impact of "intermediaries" that assist the author, known as accomplices [35]. By doing so, the authorities prove to create a comprehensive legal framework, aimed at establishing high standards for countering identity-related criminal activity.

On the other hand, section 1030 of the U.S.C. could be equally applicable, as it covers computer-focused fraud and hacking [36], mirroring the Computer Misuse Act 1990 from the United Kingdom [30]. The nexus is represented, chiefly, by referring in a couple of the prohibited acts to the condition to "affect the interstate of foreign commerce" [36, s. (a) (6) (A), s. (a) (7)].

Moreover, when it comes to protecting personal data in the context of financial or credit fraud, it has been concluded other federal laws can be applicable as well [37]: The Gramm-Leach-Bliley Act [38], The Fair Credit Reporting Act [39], The Credit Repair Organizations Act [40], the Federal Trade Commission Act [41], The Consumer Financial Protection Act of 2010 [42]. Thus, practical cases can be subject to multiple regulations at the same time. On these grounds, synthetic identity theft does not benefit from an individual and explicit incrimination, but could be covered by existing laws. However, some authors [43] believe risks are still present due to the restrictive privacy laws that limit financial institutions "to share information about synthetic identities" and subsequently, allow the perpetrators to simply change the institution and repeat the fraudulent scheme. Thus, current

"laws and agencies that are designed to help consumers also make it easier for the perpetrators to navigate and manipulate the financial system".

4. Interconnectivity and impact on personal data protection

The intrinsic relationship between synthetic identity theft and personal data relates to its unlawful use in order to "gain a financial advantage and other benefits" [6, p. 2]. To add to that, it was highlighted that the link between identity theft and personal data breaches is almost inextricable because PII is "a prerequisite to perpetrate the crime" and subsequently, "data breaches appear to be the primary source" for obtaining it [44]. However, data breaches can also be an effect of identity theft or fraud, especially when it comes to financial or health data, as per the last European Data Protection Board's guidance on data breaches' notification [45].

To analyse this in more detail, given the "personal data breach" definition from the EU and UK General Data Protection Regulation [1, Art. 4], [2, Art. 4], almost all of the possible forms are checked by synthetic identity theft: access, disclosure, transmission, storage, and the essential one, alteration. Furthermore, it has been previously identified that the mechanism sitting behind synthetic identity theft can be summed up to matching valid (stolen) social security numbers with fictious personal data "derived from one or more individuals such as name, address, date of birth, or any other information necessary to apply for any line of credit" [46]. To continue, right after the GDPR enforcement, a study has reached the conclusion that EU data protection rules have strengthened at an opportune moment for combatting the increasing number of cyber threats that lead to data breaches [47].

The nexus between synthetic identity theft and data breaches was highlighted by the European Data Protection Board as well, classifying the former as social engineering attacks. In its response to the public consultations regarding data breach notifications, the Board has confirmed the financial interests of the criminal committing synthetic identity theft, defining its purpose as "to open fraudulent accounts and make fraudulent purchases" [48]. However, regardless of the specific scope, a quick analysis of Recital 75 of the GDPR [1][2] sheds light on the relevance of identity theft on this subtopic – a processing activity that is probable to lead to identity theft means "a risk to the rights and freedoms of natural persons". On these grounds, to exemplify, such a risk will be taken into account for audits to the organisation, for evaluating the maturity of the privacy program and even for assessing the impact of data breaches.

At the same time, as explained in [16], synthetic identity theft commences with a data breach that allows personally identifiable information (PII) to be consequently unlawfully collected and shared in dark web markets. However, this PII is rather used for synthetic identity theft, instead of more direct identity-focused offenses such as payment card fraud. This was referred to as "non-ransomware data breaches", especially as the person whose information was paired with fictious details does not generally experience any financial harm. Thus, the alarmingly dangerous aspect points to the substantial difficulty to track fraudulent uses of leaked PII after data breaches, in the context where "PII relating to nearly every American consumer is already available on the dark web from multiple breaches". In my opinion, assembling the above opinions creates, in the ecosystem of synthetic identity theft, a cyber vortex where data breaches represent both the cause and effect.

On the same note, another study has emphasized that PII collected upon data breaches is generally not used in order to cause economic harm to the data subject, as "the market for consumer PII is saturated". In this context, committing synthetic identity fraud turns was not harming specific individuals, but for true identity theft or perhaps, state surveillance [16, p. 51].

As a response, regulators have established legal obligations on entities facing data breaches. The UK [2] and EU GDPR [1] are clear on that aspect, comprehensively explaining the cases when the Supervisory Authority and the data subjects must be notified at Art. 33 and 34. However, the US is more challenging. There is no such law at federal level, but states have began addressing this since

2003, commencing with California. As a confirmation of their importance, a study from 2020 has identified "the potential criminal harm of identity theft as their main rationale for the duty to notify" [44].

5. Conclusions

All in all, synthetic identity theft is part of a larger sphere from the field of cybercrimes and it becomes a growing problem for more sectors nowadays, both private and public. It is even more concerning that the impact results in harm for both natural persons and businesses, yet action and legal measures are not effectively in place at this point. There is plenty of space for evolution and in my opinion, prevention and protection need an adequate legal background for efficient enforcement.

It is clear that fraudulent schemes, especially in the digital realms, will not cease to occur and on the contrary, they will find new methods for staying "out of sight" as long as possible, taking advantage of any legal lacunae. Therefore, I believe more attention should be given to synthetic identity theft due to its peculiarities and in particular, its apparently harmless disguise. I would also find it useful and interesting to be able to identify more studies (including empirical research) on this progressive topic.

References

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

[2]. Retained Regulation (EU) 2016/679 of the European Parliament and of the Council (UK GDPR).

[3]. Police Executive Research Forum, "New National Commitment required: The Changing Nature of Crime and Criminal Investigations," Washington, D.C., USA, Jan. 2018. Accessed: Mar. 15, 2023. [Online]. Available: https://centerforimprovinginvestigations .org/wp-content/uploads/2018/04/20180000-The-Changing-Nature-of-Crime-and-Criminal-Investigations-Police-Executive-Research-Forum.pdf.

[4]. ENISA, "The year in review: ENISA Threat Landscape," Greece, Nov. 2022. Accessed: Mar. 6, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[5]. W. Bracker, S. Goeringer and S. Krauss, "Fraud Prevention and Privacy Law: Emerging Conflicts Between Privacy Law and Fraud Prevention," presented at the *SCTE ISBE Cable-Tec Expo*, Denver, CO, USA, Oct. 13-16, 2020.

[6]. ENISA, "Identity theft: ENISA Threat Landscape," Greece, Oct. 2020. Accessed: Mar. 3, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-identity-theft.

[7]. J. Bandler and A. Merzon, *Cybercrime investigations: A comprehensive resource for everyone*. Boca Raton, FL, USA: CRC Press, 2020.

[8]. AuthenticID, "2023 State of Identity Fraud," 2023. Accessed: Mar. 20, 2023. [Online]. Available: https://www.authenticid.com/2023-state-of-identity-fraud-report/.

[9]. S. Marchetti, "Rolling in the deep(fakes)," *Bank of Italy Occasional Paper*, no. *668*, Feb. 2022. Accessed: Mar. 3, 2023. [Online]. Available: doi:10.2139/ssrn.4032831.

[10]. J. Davis, "The real victim in health data breaches? Patients' medical identities," *HealthcareITNews,* Oct. 29, 2018. Accessed: Mar. 28, 2023. [Online]. Available: https://

www.healthcareitnews.com/news/real-victim-health-data-breaches-patients-medical-identities.

[11]. Federal Reserve Banks, "Defining Synthetic Identity Fraud," 2021. Accessed: Mar. 29, 2023. [Online]. Available: https://fedpaymentsimprovement.org/wp-content/uploads/synthetic-identity-fraud-definition-overview.pdf.

[12]. B. Richardson and D. Waldron, "Fighting back against synthetic identity fraud," *McKinsey on Risk,* no. 7, Jan. 2019. Accessed: Mar. 13, 2023. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/fighting-back-against-synthetic-identity-fraud.

[13]. C.J. Hoofnagle, "Identity Theft: Making the Known Unknowns Known," *Harvard Journal of Law & Technology*, vol. 21, no. 1, pp. 97-122, Fall 2007. Accessed: Mar. 13, 2023. [Online]. Available: https://ssrn.com/abstract=969441.

[14]. D. Rebovich and J.M. Byrne, Eds., *The New Technology of Financial Crime: New Crime Commission Technology, New Victims, New Offenders, and New Strategies for Prevention and Control*. Routledge. 2023.

[15]. Federal Reserve, "Mitigating Synthetic Identity Fraud in the U.S. Payment System," 2020. Accessed: Mar. 9, 2023. [Online]. Available: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf.

[16]. D.W. Opderbeck, "Cybersecurity and Data Breach Harms: Theory and Reality" in Seton Hall University School of Law Legal Studies Research Paper Series, Aug. 2022, p. 54. Accessed: Mar. 29, 2023. [Online]. Available: doi.org/10.2139/ssrn.4187263.

[17]. United Nations Office on Drugs and Crime, *Handbook on Identity-related Crime*, 2011. Accessed: Apr. 9, 2023. [Online]. Available: https://www.unodc.org/documents/congress/background-information/Corruption/Handbook_on_Identity-related_Crime_ENG.pdf.

[18]. Coronavirus Aid, Relief, and Economic Security Act (CARES Act), Pub. L. No. 116-136, H.R.748. 2020 [Online]. Available: https://www.congress.gov/bill/116th-congress/house-bill/748/text.

[19]. *Two Men Who Allegedly Used Synthetic Identities, Existing Shell Companies, and Prior Fraud Experience to Exploit Covid-19 Relief Programs Charged in Miami Federal Court*, United States Attorney's Office – Southern District of Florida, Aug. 28, 2020. Accessed: Apr. 9, 2023. [Online]. Available: https://www.justice.gov/usao-sdfl/pr/two-men-who-allegedly-used-synthetic-identities-existing-shell-companies-and-prior-0.

[20]. Pandemic Response Accountability Committee, "Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs," Jun. 2022. https://www.pandemicoversight.gov/media/file/identity-fraud-capping-report.

[21]. United States v Rose, D Ariz, Aug. 22, 2006, CR06-0787PHX.

[22]. Federal Reserve, "Synthetic Identity Fraud Mitigation Toolkit," 2022. Accessed: Apr. 2, 2023. [Online]. Available: https://fedpaymentsimprovement.org/synthetic-identity-fraud-mitigation-toolkit/.

[23]. Federal Reserve, "Protecting Your Kids from Synthetic Identity Fraud", 2022. Accessed: Apr. 2, 2023. [Online]. Available: https://fedpaymentsimprovement.org/wp-content/uploads/protect-kids-from-synthetic-identity-fraud.pdf.

[24]. Convention on Cybercrime, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004).

[25]. F. D. Ciccio, "Comparison of Identity Theft in Different Countries," 2014. [Online]. Available: https://courses.cs.ut.ee/MTAT.07.022/2014_fall/uploads/Main/francesco-report-f14.pdf.

[26]. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement [2019] OJ L 188/67.
[27]. UK House of Lords, "Fighting Fraud: Breaking the Chain," Fraud Act 2006 and Digital Fraud Committee Report of Session 2022-23, HL Paper 87, 2022. Accessed: Mar. 27, 2023. [Online]. Available: https://publications.parliament.uk/pa/ld5803/ldselect/.
[28]. UK Fraud Act 2006 (2006, Nov. 8). Accessed: Apr. 10, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/2006/35/contents.
[29]. UK Computer Misuse Act 1990 (1990, Jun. 29). Accessed: Apr. 10, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18/contents.
[30]. UK Identity Documents Act 2010 (2010, Dec. 21). Accessed: Apr. 10, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/2010/40.
[31]. S.R. Ahmed, "Identity Crime Legislation in the United States, Canada, Australia and the United Kingdom," in *Preventing Identity Crime: Identity Theft and Identity Fraud*, Brill|Nijhoff, 2020, ch. 6, pp. 252-542. https://doi.org/10.1163/9789004395978_007.
[32]. UK Cabinet Office and Government Digital Service, "Guide: How to prove and verify someone's identity," Jan. 9, 2023. Accessed: Apr. 10, 2023. [Online]. Available: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity.
[33]. U.S. Code, Title 18, pt. I, ch. 47, section 1028.
[34]. Paul Newmann, "Identity Theft: A Growing Problem," The Bill Blackwood Law Enforcement Management Institute of Texas, Denison, TX, USA, 2018. Accessed: Apr. 3, 2023. [Online]. Available: https://shsu-ir.tdl.org/bitstream/handle/20.500.11875/2452/1767.pdf?sequence=1&isAllowed=y.
[35]. Congressional Research Service, "Accomplices, Aiding and Abetting, and the Like: An Overview of 18 U.S.C. § 2," R43769, 2020. Accessed: Apr. 3, 2023. [Online]. Available: https://sgp.fas.org/crs/misc/R43769.pdf.
[36]. U.S. Code, Title 18, pt. I, ch. 47, section 1030.
[37]. U.S. Government Accountability Office, "Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud," GAO-17-254, Mar. 2017. Accessed: Apr. 3, 2023. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1031224.pdf.
[38]. U.S. Gramm-Leach-Bliley Act (GLBA) of 1999. 15 U.S.C, § 6801-6809, § 6821-6827.
[39]. U.S. Fair Credit Reporting Act (FCRA) of 1970. 15 U.S.C, § 1681-1681x.
[40]. U.S. Credit Repair Organizations Act (CRA) of 1996.15 U.S.C. § 1679-1679j.
[41]. U.S. Federal Trade Commission Act (FTC Act) of 1914. 15 U.S.C. § 41-58, as amended.
[42]. U.S. Consumer Financial Protection Act of 2010. 12 U.S.C. § 5301-5641.
[43]. IBM, "Synthetic identity fraud: Can I borrow your SSN?: Who else might be using your Social Security number and why?," Armonk, NY, USA, Mar. 2015. Accessed: Apr. 9, 2023. [Online]. Available: http://www.turnkeyrisk.com/images/whitepapers/Can-I-borrow-your-SSN.pdf.
[44]. F. Bisogni and H. Asghari, "More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws," *Journal of Information Policy*, vol. 10, pp. 45-82, May 2020. Accessed: Apr. 9, 2023. [Online]. Available: doi:10.5325/jinfopoli.10.2020.0045.
[45]. Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, Adopted 28 March 2023. Accessed: Mar. 13, 2023. [Online]. Available: https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

[46]. N. L. Piquero, A. R. Piquero, S. Gies, B. Green, A. Bobnis and E. Velasquez, "Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders", *Victims & Offenders*, vol. 16, no. 3, pp. 444-463, 2021. Accessed: Apr. 8, 2023. [Online]. Available: doi:10.1080/15564886.2020.1826023.

[47]. European Commission, "Trends in electronic identification: An overview: Value Proposition of eIDAS eID," COM/DIGIT.D3/2017/01-035, 2018. Accessed: Apr. 18, 2023. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/78549570/Trends%20report%20on%20electronic%20identification_for%20publication_v.1.1.pdf?version=1&modificationDate=1551198712785&api=v2.

[48]. dataTENET, Response to the public consultation "Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on January 14, 2021, Version 1.0", Mar. 1, 2021. Accessed: Apr. 18, 2023. [Online]. Available: https://edpb.europa.eu/sites/default/files/public_consultation_replies/mail_edpb_02_03_response_to_the_public_consultation_guidelines_012021_.pdf.