



Empowering FinTech with Fully Homomorphic Encryption: A Revolutionary Approach

Table of Contents

Abstract 1

Challenges..... 2

 Regulatory Compliance.....2

 Cybersecurity Risks3

 Consumer Trust And Privacy Concerns5

Solutions 5

 Advanced Encryption Techniques5

 Protecting Consumer Data6

Benefits 7

 Regulatory Compliance.....7

 Cybersecurity Advantages.....8

 Cyber Crimes Investigations9

The Impact of Scalable Computing on Privacy-Enhancing Technologies in FinTech 10

Conclusion 11

Sources 12

Abstract

In the ever-evolving realm of Financial Technology (FinTech), the very *concept* of FinTech marks a revolutionary advancement, reshaping the fundamental mechanics of financial transactions. These innovative protocols, operating autonomously, execute the intricacies of financial agreements embedded within their code. By eliminating traditional intermediaries, FinTech optimizes transaction processes, enhancing efficiency, reducing costs, and fostering trust among participants.

Central to FinTech is blockchain technology, which provides a decentralized ledger that securely records financial agreements, mitigating the risks of tampering and uncertainties inherent in conventional methods. This transformative system is driving various sectors, including finance, towards a transparent and automated economy.

However, the progress of FinTech is hindered by challenges in data privacy, analogous to those encountered in sectors such as healthcare where the management of sensitive information is paramount. Here, Fully Homomorphic Encryption (FHE) emerges as a potential solution. By enabling

computations on encrypted data without decryption, FHE fortifies FinTech against privacy breaches while facilitating essential analytics and data exchange crucial for advancing digital transactions.

The practical application of FHE within FinTech has historically faced barriers due to its intensive computational requirements. Yet, the advent of Cornami's FracTLcore™ computing fabric technology presents a promising solution. This scalable and reconfigurable computing architecture is purpose-built to meet the rigorous demands of FHE, surpassing traditional computational limitations and offering a massively scalable and adaptable computing framework. This innovation signifies the transformation of a theoretically robust security measure into a commercially viable reality for FinTech, potentially ushering in a new era of secure and efficient data sharing.

This paper recognizes the practical challenges hindering the widespread adoption of FHE, particularly its computational demands. It proposes that innovative post-von Neumann computing architectures, such as Cornami's FracTLcore® Compute Fabric, hold the key to overcoming these obstacles. By providing the necessary computational power, these technologies make FHE a viable option for organizations dealing with and executing FinTech solutions.

Through this whitepaper, we aim to explore the intersection of FinTech's role in data exchange, the imperative for stringent cybersecurity, and the advanced computing solutions poised to redefine data transaction security. Our goal is to chart a prospective path, revealing how to harness the power of data amidst the intricacies of privacy and security in an increasingly data-centric FinTech landscape.

Challenges

Regulatory Compliance

Navigating the intricate landscape of data sharing in the FinTech industry presents a formidable challenge, particularly when it comes to reconciling the drive for innovation with adherence to stringent data protection regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These regulatory frameworks, established to safeguard individuals' privacy rights and personal data, impose rigorous requirements on FinTech firms aiming to share data across borders while maintaining compliance with diverse legal mandates.

The GDPR, implemented in 2018, represents a landmark regulation governing the processing and transfer of personal data within the European Union (EU) and the European Economic Area (EEA). It mandates that organizations processing personal data must ensure lawful and transparent processing, obtaining explicit consent from data subjects for data processing activities [1]. Furthermore, the GDPR imposes strict restrictions on the transfer of personal data outside the EEA, necessitating the implementation of appropriate safeguards to protect data subjects' rights and freedoms [2].

Similarly, the CCPA, enacted in 2020, confers California residents with significant rights over their personal information held by businesses. These rights include the right to know what personal information is being collected, the right to opt out of the sale of personal information, and the right to

access and delete personal information upon request [3]. Notably, the CCPA applies to businesses meeting specific criteria, irrespective of their physical presence in California, thereby extending its jurisdictional reach to FinTech entities operating beyond the state's borders [4].

For FinTech firms engaged in cross-border data-sharing endeavors, compliance with the GDPR and CCPA poses a formidable challenge. Such compliance necessitates the implementation of robust data protection mechanisms, encompassing encryption, anonymization, and data minimization strategies, to safeguard personal data while facilitating lawful data-sharing activities [5]. Additionally, these firms must grapple with the intricacies of international data transfers, ensuring adherence to the GDPR's stringent requirements governing the export of personal data outside the EEA [6].

The source of the challenge lies in striking a delicate balance between harnessing data for innovation and growth while upholding the stringent data protection standards enshrined in regulations like the GDPR and CCPA. Non-compliance with these regulations carries significant repercussions, including hefty fines and reputational damage, underscoring the imperative for FinTech firms to adopt a proactive approach to data governance and compliance.

Cybersecurity Risks

Safeguarding financial information from cyber threats and data breaches demands robust security measures, given the highly interconnected nature of data sharing within the FinTech ecosystem. The proliferation of digital transactions and the increasing reliance on cloud-based services and third-party integrations amplify the risks associated with cyberattacks, making it imperative for FinTech firms to adopt comprehensive cybersecurity strategies [7].

One significant cybersecurity risk confronting FinTech firms is the threat of data breaches, wherein malicious actors gain unauthorized access to sensitive financial information. According to the Identity Theft Resource Center (ITRC), there were 1,862 reported data breaches in the United States alone in 2020, exposing over 300 million records [8]. These breaches not only result in financial losses but also erode consumer trust and confidence in FinTech platforms.

Additionally, FinTech firms are vulnerable to various forms of cyber threats, including malware, ransomware, phishing attacks, and distributed denial-of-service (DDoS) attacks. Malware, such as viruses and trojans, can infiltrate FinTech systems, compromising data integrity and confidentiality. Ransomware attacks, where cybercriminals encrypt sensitive data and demand ransom payments for decryption, pose a significant threat to FinTech firms, potentially disrupting operations and causing financial harm [9].

Phishing attacks represent another prevalent cybersecurity risk, wherein cybercriminals impersonate legitimate entities to deceive users into divulging confidential information, such as login credentials and financial details. With the increasing sophistication of phishing tactics, FinTech firms must implement robust authentication mechanisms and user education programs to mitigate the risk of phishing attacks [10].

Furthermore, the reliance on third-party vendors and service providers introduces additional cybersecurity challenges for FinTech firms. While outsourcing certain functions can enhance operational efficiency, it also expands attack surfaces and introduces potential vulnerabilities. FinTech firms must conduct thorough due diligence on third-party vendors, assess their security posture, and implement contractual safeguards to mitigate the risks of data breaches and security incidents [11].

FinTech firms are increasingly targeted by cybercriminals due to the high-value financial transactions and sensitive customer information they handle. Implementing multi-layered security measures is essential to protect against these threats. This approach includes encryption, intrusion detection systems, access controls, and comprehensive employee training programs. Collaboration with cybersecurity experts and participation in information-sharing initiatives further enhances threat intelligence and defense capabilities against evolving cyber threats.

Key Components of Multi-Layered Security:

1. **Encryption:** Secures data in transit and at rest, making it unreadable to unauthorized individuals.
2. **Intrusion Detection Systems (IDS):** Monitor network and system activities for malicious activities or policy violations.
3. **Access Controls:** Ensure that only authorized individuals can access sensitive information, based on their roles.
4. **Employee Training Programs:** Educate employees on recognizing and responding to cybersecurity threats like phishing attacks.

Benefits of Multi-Layered Security:

1. Provides comprehensive coverage against a wide range of threats by implementing various security controls at different levels (network, endpoints, applications, and users).
2. Enhances the overall security posture of the system, making it difficult for cybercriminals to infiltrate.
3. Offers adaptability to evolving threats, allowing for the integration of new security controls as threats and technologies develop. [12]

Collaboration and Information Sharing:

Collaborating with cybersecurity experts and participating in information-sharing initiatives are crucial for staying ahead of emerging cyber threats. These partnerships facilitate the exchange of threat intelligence, enabling FinTech firms to adapt their security measures in response to new information about potential vulnerabilities and attack methods.

Implementing a multi-layered security approach, combined with ongoing collaboration and information sharing, empowers FinTech firms to protect themselves and their customers from the increasingly sophisticated and diverse range of cyber threats they face today [13].

Overall, addressing cybersecurity risks is paramount for FinTech firms to maintain the integrity, confidentiality, and availability of financial information in an increasingly interconnected and digitally driven ecosystem [13].

Consumer Trust and Privacy Concerns

Maintaining consumer trust while respecting privacy preferences poses significant challenges, especially given the need to balance personalized services with user data boundaries. Research indicates that ethical considerations, including bias, discrimination, privacy, transparency, justice, ownership, and control, are crucial in the intersection of big data, AI, and customer trust within FinTech. Companies are advised to safeguard customer data, comply with data protection laws, and promote corporate digital responsibility to build trust. Practical suggestions include employing encryption techniques, ensuring transparency in data collection and usage, providing customers with opt-out options, and training staff on data protection policies [14].

Balancing innovation with consumer protection in FinTech requires addressing significant challenges, such as the pace of technological breakthroughs outpacing regulatory development, data breaches, ethical decision-making, and enhancing consumer education and awareness. Strategies for responsible FinTech innovation include embedding privacy and security measures from the outset, fostering collaboration, enhancing transparency, empowering users, and investing in continuous education and training for staff [15].

Addressing data privacy in the digitized world is pivotal, with FinTech at the core of major security concerns. Implementing the latest security practices, such as multi-factor authentication, biometric authorization, and regular risk assessments, is essential for FinTech apps. Additionally, transparency about data collection, comprehensive terms of use, privacy policies, and regulatory compliance helps build authority and gain trust. Educating users about the app's functionalities and integrating safety measures into the user experience (UX) are also recommended practices for fostering trust in FinTech solutions [16].

For a comprehensive expansion on building and maintaining trust among users in the FinTech sector, it is imperative to delve into the complex relationship between technological innovation and ethical standards, regulatory compliance, and the imperative of protecting consumer data privacy.

Solutions

Advanced Encryption Techniques

Implementing Fully Homomorphic Encryption (FHE) offers FinTech firms a groundbreaking way to ensure data privacy and security, enabling secure computation on encrypted data. This means that companies can perform necessary analytics while the data remains encrypted, ensuring that sensitive information is

never exposed, even during the data-sharing process. This capability meets stringent regulatory requirements without compromising the confidentiality of sensitive information.

The concept of FHE is considered by many, including the United States Department of Defense, as the "holy grail of encryption". FHE allows for operations to be performed on encrypted data, generating encrypted results that, when decrypted, match the results of operations performed on the plaintext. This level of encryption provides a robust foundation for privacy-preserving computation, ensuring data security at rest, in transit, and during processing. FHE addresses the critical challenge of protecting data not just when it is stored or being sent over networks but more importantly, while it is being used or processed. The significance of FHE lies in its ability to enable the use of untrusted networks and enhance data privacy by ensuring that data or models remain encrypted throughout the computation process.

Initially presented by Craig Gentry in 2009, FHE has evolved through various schemes, including the Cheon-Kim-Kim-Song (CKKS) scheme which is efficient for floating point calculations, and commonly used in machine learning algorithms. FHE schemes are based on complex mathematical constructs, particularly lattice and Learning with Errors (LWE) problems, which are considered difficult to solve and likely resistant even to quantum computing attacks. This makes FHE a quantum-safe solution, providing a strong cryptographical guarantee of the security of data during processing, a critical protection that traditional encryption schemes do not address [17].

Yet, the practical application of FHE has been limited by its significant computational overhead. Recent research efforts, including those by NYU Tandon School of Engineering, are focused on developing specialized hardware accelerators to make FHE computation more feasible for practical applications. These efforts aim to dramatically decrease the performance penalty incurred by FHE computations and accelerate FHE calculations to approach the performance levels of current unencrypted data processing [18].

Traditional computing systems often struggle to efficiently handle the complex calculations required for FHE. This is where Cornami's FracTLcore® Scalable and Reconfigurable Computing Fabric technology comes into play. Cornami's architecture is specifically designed to tackle the computational challenges posed by advanced cryptographic techniques such as FHE.

For FinTech applications, the adoption of FHE can transform how data is securely managed, enabling new levels of privacy and security for financial transactions and customer data. As FHE technology continues to mature and becomes more accessible, it holds the potential to redefine the standards for data privacy and security in the FinTech industry and beyond, and Cornami's Scalable Computing Fabric technology offers massive hardware acceleration capabilities, enabling the rapid processing of encrypted data while maintaining high levels of privacy and security.

Protecting Consumer Data

In the realm of FinTech, protecting consumer data has emerged as a critical undertaking, notably through the utilization of FHE. This technology ensures that sensitive financial information remains encrypted throughout its lifecycle, thus establishing a trust foundation by showcasing a commitment to user privacy

alongside the delivery of personalized services. The significance of leveraging FHE lies in its ability to perform computations on encrypted data, offering a robust security measure that doesn't compromise the data's confidentiality during analysis [15], [19], [20].

Addressing cybersecurity comprehensively, FinTech firms are encouraged to implement a variety of protective measures. Regular risk assessments, Multi-Factor Authentication (MFA), and robust encryption practices are pivotal in safeguarding consumer information against unauthorized access. Furthermore, establishing a well-defined incident response plan and fostering a culture of cybersecurity awareness among employees are vital strategies for mitigating risks associated with data breaches and cyberattacks. These practices not only enhance security but also play a crucial role in maintaining compliance with regulatory standards, such as GDPR and PCI DSS, underscoring the industry's commitment to consumer protection [19].

The evolution of FinTech services also necessitates a focus on ethical considerations and consumer education. FinTech companies must integrate ethical decision-making processes, promote data literacy, and ensure transparency in their operations. These efforts should be complemented by promoting collaboration with regulators and industry peers to share best practices and insights, thus enabling the FinTech ecosystem to navigate the complexities of digital finance responsibly [15].

The digital transformation within banking and FinTech underscores the transition towards cloud-native platforms, highlighting the role of digital strategies in enhancing data security. By moving to the cloud, financial institutions can leverage advanced technologies to ensure safer payment processes and better manage cybersecurity threats. The adoption of identity verification technologies and comprehensive digital identification procedures further supports the endeavor to protect consumer data in an ever-evolving digital landscape [20].

The FinTech industry's approach to consumer data protection is multifaceted, intertwining advanced encryption technologies like FHE with a broad spectrum of cybersecurity measures and ethical practices. By prioritizing consumer safety and adhering to regulatory standards, FinTech firms can harness the full potential of data-driven innovation while safeguarding individual privacy and fostering a sustainable and inclusive financial future [15], [19], [20].

Benefits

Regulatory Compliance

FHE significantly aids FinTech firms in maintaining regulatory compliance while managing sensitive data. FHE enables secure computation on encrypted data, thus allowing companies to analyze and gain insights from data without the need to decrypt it. This ensures adherence to stringent data protection regulations such as the General Data Protection Regulation (GDPR) while still leveraging data for valuable insights [21], [22].

The adoption of FHE and similar privacy-preserving technologies is becoming increasingly vital as FinTechs navigate a complex web of regional and international data protection laws. For instance, the GDPR in the EU places heavy emphasis on the lawful processing of personal data, requiring FinTech organizations to carefully choose the correct basis for data processing, such as consent, legitimate interest, or performance of a contract. FinTech firms must ensure transparency, obtain proper consent, and respect the privacy rights of individuals, including access, rectification, erasure, and the right to object to data processing [22].

Likewise, the compliance checklist for FinTechs highlights the importance of adhering to a patchwork of regulations across different regions, including emerging laws in states like Virginia and California. This emphasizes the need for FinTech companies to stay informed and agile, adapting their data protection strategies to comply with both current and upcoming regulations. Ensuring compliance not only protects against steep penalties but also reinforces customer trust and loyalty by demonstrating a commitment to privacy and security [21].

In addition to legal compliance, adopting a privacy-aware culture and integrating principles of privacy by design into FinTech operations can further strengthen a company's stance on data protection. This involves embedding privacy considerations into the development process of FinTech services, ensuring end-to-end security, and being transparent about data handling practices. Such an approach is aligned with both ethical standards and consumer expectations, ultimately contributing to a more trustworthy and sustainable FinTech ecosystem.

Leveraging FHE and closely adhering to data protection laws and principles are critical steps for FinTech companies aiming to ensure regulatory compliance, safeguard consumer data, and maintain a competitive edge in the rapidly evolving digital finance landscape.

Cybersecurity Advantages

Incorporating FHE into the cybersecurity strategies of FinTech companies significantly enhances data protection by enabling computations on encrypted data. This innovative approach minimizes the risk of exposing sensitive financial information by reducing potential attack vectors and reinforcing the security infrastructure within the FinTech sector. The adoption of FHE is part of a broader set of cybersecurity practices critical for safeguarding digital financial services.

Key components of a comprehensive cybersecurity strategy in the FinTech industry include conducting thorough risk assessments, implementing multi-factor authentication (MFA), enforcing strong encryption protocols, and developing robust incident response frameworks. Regular risk assessments help identify and mitigate vulnerabilities, MFA adds an essential layer of security, and encryption of data in transit and at rest protects against unauthorized access. An effective incident response plan ensures that FinTech firms can quickly react to and recover from cyber incidents [19].

Continuous monitoring and testing of FinTech systems play a vital role in early vulnerability detection and the maintenance of security measures. Educating employees about cybersecurity best practices is equally important, as it empowers staff to recognize and prevent potential cyber threats. Collaborative

efforts among FinTech companies, regulatory bodies, and cybersecurity experts facilitate the exchange of threat intelligence and the development of industry-wide security standards [19].

The integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity operations marks a significant advancement in threat detection and response capabilities. These technologies enable the analysis of large datasets to identify unusual patterns and behaviors that may indicate a security threat, allowing for proactive and efficient cybersecurity measures [19].

FinTech companies also face challenges such as managing insider threats and third-party risks; and balancing robust security with a seamless user experience. Techniques such as encryption, comprehensive cybersecurity training, detailed incident response strategies, and strategic partnerships are employed to address these challenges and mitigate cybersecurity risks. These measures aim to protect sensitive financial data, comply with regulatory requirements, and preserve consumer trust in digital financial services [23], [24].

Blockchain technology further strengthens cybersecurity in FinTech by offering a secure, transparent, and immutable platform for conducting financial transactions. Its decentralized architecture and consensus mechanisms reduce the risk of data breaches and unauthorized data manipulation, contributing to the overall integrity and security of FinTech platforms [24].

As the FinTech industry navigates an increasingly complex cyber threat landscape, leveraging FHE, alongside comprehensive cybersecurity practices and the adoption of cutting-edge technologies like AI and blockchain, is crucial for protecting financial data and ensuring the resilience of the digital financial ecosystem.

Cyber Crimes Investigations

FHE is revolutionizing the field of financial crime investigation by enabling analysis of encrypted data, thus maintaining the privacy and security of sensitive financial information. FHE's capacity to allow for complex computations on encrypted data without decryption eliminates the risk of data exposure during the investigation process. This breakthrough technology is a game-changer in enforcing fraud detection and flagging suspicious activities, all while adhering to data protection standards.

The rise of Artificial Intelligence (AI) in combating financial crimes is noteworthy. AI's ability to sift through vast amounts of data from a variety of sources—including public records, online databases, and even the deep web—transforms the landscape of financial crime investigations. AI technologies deploy sophisticated algorithms to detect unusual patterns of behavior, identify relationships, and spot irregularities in financial transactions. These capabilities significantly strengthen efforts to combat money laundering, identity theft, and various forms of fraud, making AI an indispensable tool in the arsenal against financial crimes [25].

The U.S. Secret Service's role in protecting the financial infrastructure of the nation underscores the importance of adapting to technological advancements in combating financial and cyber crimes. Their

focus has shifted towards addressing sophisticated crimes such as credit card fraud, wire fraud, computer network breaches, and other cyber-enabled financial crimes, reflecting the evolving nature of financial crimes in the digital age. The Secret Service's investigative efforts encompass a broad spectrum of financial crimes, showcasing the critical need for innovative solutions like FHE and AI in safeguarding financial systems and sensitive information from criminal exploitation [26].

In the context of financial crime investigations, technologies like FHE and AI represent a paradigm shift towards more secure, efficient, and effective investigation methodologies. As financial institutions and investigative agencies integrate these technologies into their operations, the ability to analyze encrypted data securely and leverage AI for anomaly detection will play a pivotal role in mitigating risks associated with financial crimes. The advancements in these technologies not only enhance the security and privacy of financial data but also significantly improve the detection and prevention of financial crimes, contributing to the overall resilience of financial systems against the threats posed by cybercriminals.

The ongoing development and application of FHE and AI in financial crime investigations highlight the necessity for continuous innovation and collaboration among technology providers, financial institutions, and law enforcement agencies. As these technologies evolve, so too will the strategies employed by criminals, necessitating a proactive and adaptive approach to financial crime prevention and investigation.

The Impact of Scalable Computing on Privacy-Enhancing Technologies in FinTech

The advancement of privacy technologies in the FinTech sector is vital for safeguarding sensitive financial data. Innovations like Cornami's scalable and reconfigurable FracTLcore® Compute Fabric are pivotal in meeting the high computational demands of FHE. This scalable computing architecture facilitates real-time encrypted processing of financial data while preserving the highest security standards.

This architecture is scalable, reconfigurable, and versatile, catering to the diverse computational needs inherent in various privacy technologies within the FinTech industry. It ensures the efficient functioning of intricate algorithms essential for FHE and allows for the integration of FHE with synergistic technologies such as Zero Knowledge Proofs (ZKP) and Privacy-Preserving Machine Learning (PPML). This integration fosters robust solutions that process sensitive financial information efficiently without compromising security.

By optimizing the computational aspects, Cornami's FracTLcore® Compute Fabric enables complex computations on encrypted data to be performed rapidly and securely, a crucial requirement for financial institutions. The FinTech sector, therefore, stands to gain from the dual benefits of high-performance computing and stringent data privacy measures.

With such technological advancements, FinTech organizations can explore new horizons for securely handling and analyzing extensive financial data sets. This is critical not only for preserving consumer

confidence but also for advancing financial analytics and service personalization. The FracTLcore® Compute Fabric by Cornami signifies a significant leap in applying compute-intensive privacy technologies, heralding the development of more sophisticated and secure financial data processing systems.

Conclusion

In analyzing the transformative impact of FHE in FinTech, we recognize its critical role in securing sensitive financial data and proprietary insights. FinTech entities employ FHE to analyze and exchange encrypted data safely, negating the necessity for decryption, thereby enhancing protection against cyber-attacks, and ensuring compliance with stringent financial regulations like the GDPR and PCI DSS.

In FinTech, where data security is of utmost importance due to the confidential nature of financial data, FHE facilitates secure data analysis and sharing. This is vital for the development of collaborative efforts in financial innovation while safeguarding client and proprietary information. The implementation of FHE in FinTech data systems introduces myriad advantages. Beyond meeting regulatory compliance, it enables joint ventures in financial research, risk assessment, and customer service enhancement. The computational intensity of FHE poses challenges; however, advances in hardware accelerators and algorithmic efficiency are broadening its applicability in the FinTech space.

The prospective influence of FHE on FinTech, particularly when integrated with scalable computing solutions from Cornami, is significant. Cornami's scalable computing framework addresses the intense computational requirements of FHE, enabling swift processing of encrypted data, thus facilitating broader adoption of this technology.

By harnessing the strengths of FHE and the technological advancements from Cornami, the FinTech sector is primed to embark on a new chapter. In this chapter, paramount data privacy, fortified security, and collaborative innovation converge, driving the industry toward a secure, effective, and cooperative future.

Sources

1. Regulation (EU) 2016/679 of the European Parliament and of the Council
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
2. Regulation (EU) 2016/679, art. 44.
<https://www.legislation.gov.uk/eur/2016/679/article/44#:~:text=Article%2044General%20principle%20for%20transfers&text=All%20provisions%20in%20this%20Chapter,this%20Regulation%20is%20not%20undermined>
3. California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (2020).
<https://casetext.com/statute/california-codes/california-civil-code/division-3-obligations/part-4-obligations-arising-from-particular-transactions/title-1815-california-consumer-privacy-act-of-2018/section-1798100-general-duties-of-businesses-that-collect-personal-information#:~:text=A%20business%20shall%20not%20collect%20additional%20categories%20of%20sensitive%20personal,the%20consumer%20with%20notice%20consistent>
4. California Consumer Privacy Act, Cal. Civ. Code § 1798.140(c)(1) (2020).
<https://law.justia.com/codes/california/2022/code-civ/division-3/part-4/title-1-81-5/section-1798-140/>
5. European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679, 2020, at 19.
https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
6. European Data Protection Board, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, 2020, at 15.
https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
7. Maurer, T. and Nelson, A. 2021 - “The Global Cyber Threat”
<https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>
8. Identity Theft Resource Center - 2020 Data Breach Report
<https://www.idtheftcenter.org/post/the-itrc-2020-data-breach-report-reveals-good-and-bad-news-for-businesses-and-consumers/#:~:text=After%20a%2017%20percent%20increase,in%20breaches%20and%20consumers%20impacted.>
9. National Credit Union Administration - “Ransomware Is a Serious and Growing Threat”
<https://ncua.gov/newsroom/ncua-report/2016/ransomware-serious-and-growing-threat>
10. Proofpoint - 2024 State of the Phish Report
<https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
11. Deloitte Development LLC. – 2023- “The rising importance of third party risk management (TPRM)”
<https://www2.deloitte.com/us/en/pages/risk/articles/supply-chain-risk-management-strategies.html>

12. Avey, C. - 2023 – “The Importance of a Multi-Layered Approach to Cybersecurity”
<https://www.globalsign.com/en/blog/multi-layered-approach-cybersecurity>
13. Barnes, A. - 2022 - “Cybersecurity in FinTech: Challenges and prospects”
<https://capital.com/cybersecurity-in-FinTech>
14. Aldboush, H., Marah Ferdous, M – 2023 - “Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust”
<https://www.mdpi.com/2227-7072/11/3/90>
15. Finance Magnates – 2023 - “Data Privacy and Ethics in Fintech: Balancing Innovation with Consumer Protection” <https://www.financemagnates.com/FinTech/data/data-privacy-and-ethics-in-FinTech-balancing-innovation-with-consumer-protection/>
16. Osypenko, A. - “How to Build Trust in Your Fintech App”
<https://madappgang.com/blog/FinTech-trust/>
17. IBM Research (2022) "Fully Homomorphic Encryption" <https://research.ibm.com/topics/fully-homomorphic-encryption>
18. NYU School of Engineering – 2023 – “The Future of Fully Homomorphic Encryption - NYU Tandon researchers are developing specialized hardware accelerators for enabling computation on encrypted data”
<https://spectrum.ieee.org/fully-homomorphic-encryption>
19. Finance Magnates – 2023 - Cybersecurity in Fintech 2023: Protecting Customer Data and Financial Systems
<https://www.financemagnates.com/FinTech/data/cybersecurity-in-FinTech-2023-protecting-customer-data-and-financial-systems/>
20. England, J. - 2022 – “How fintech and banking technology is protecting data”
<https://FinTechmagazine.com/banking/how-FinTech-and-banking-technology-is-protecting-data>
21. InnReg – 2023 – “Data Protection Compliance Checklist: Stricter Rules for Fintechs”
<https://www.innreg.com/blog/data-protection-compliance-checklist-stricter-rules-for-FinTechs>
22. Legal Nodes – 2024 – “GDPR Compliance for Fintech Companies: A Comprehensive Guide”
<https://legalnodes.com/article/gpdr-compliance-FinTech>
23. Finance Magnates – 2023 – “The Changing Landscape of Cybersecurity in Fintech”
<https://www.financemagnates.com/FinTech/data/the-changing-landscape-of-cybersecurity-in-FinTech/>
24. Finance Magnates – 2023 – “Cybersecurity Trends and Challenges in the Fintech Industry”
<https://www.financemagnates.com/FinTech/data/cybersecurity-trends-and-challenges-in-the-FinTech-industry/>
25. Pribanic, E. - 2020 – “AI: The Future of Financial Crime Investigation”
<https://www.techfunnel.com/FinTech/ai-the-future-of-financial-crime-investigation/>
26. United States Secret Service, Cyber Investigations
<https://www.secretservice.gov/investigations/cyber>

Additional Resources

- Aelex – “Cybercrime and Cybersecurity: Fintech’s Greatest Challenges”
https://www.aelex.com/wp-content/uploads/2019/08/Cybercrime-and-Cybersecurity_-FinTech’s-Greatest-Challenges1.pdf
- Dr. Thomas J. Holt - Simon Fraser University - International CyberCrime Research Centre
<https://www.sfu.ca/iccrc/members/memberprofiles/thomas-j-holt.html>
Watch Guard – “Strengthening Security: The Power of Multiple Layers Against Advanced Threats”
<https://www.watchguard.com/wgrd-news/blog/strengthening-security-power-multiple-layers-against-advanced-threats>
- Congressional Research Services – 2023 – “Banking, Data Privacy, and Cybersecurity Regulation”
<https://crsreports.congress.gov/product/pdf/R/R47434/2>