



Security Breach Notice Report

An overview of the security breach notices received by SCDCA since 2019 as well as a detailed analysis of the security breach notices received in 2023.

2024

Number of Security Breach Notices Received by Industry January 2019 – December 2023

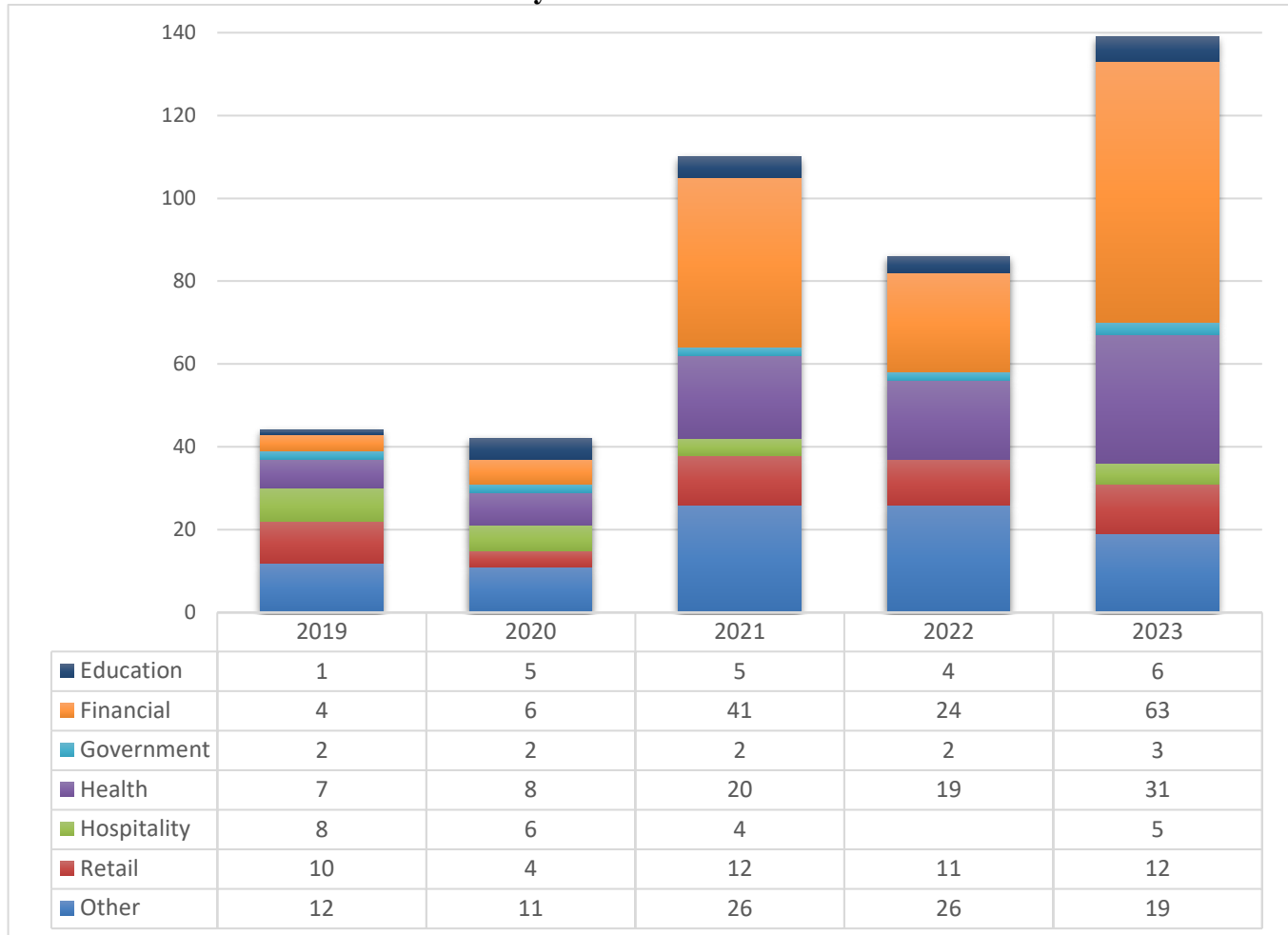


Figure 1

From January 2019 through December 2023, SCDCA received **421** breach notices: a total of one-hundred thirty-eight (138) reported by financial service providers; eighty-five (85) from healthcare organizations; forty-eight (49) breaches reported by the retail industry; twenty-three (23) from the hospitality industry; twenty-one (21) from education providers; and eleven (11) from governmental entities. SCDCA also received ninety-four (94) reports of breaches from organizations outside these six main categories.

SCDCA received 139 notices in 2023, exceeding the number of notices in 2021 (110), which was the previous highest since 2012. Prior to 2019, the average number of notices per year was 42. The notices received in 2019 (44) and 2020 (42) were in line with the average. However, the number of notices received in 2021 (110), 2022 (86), and 2023 (139) have increased the average number of notices to 59 per year for 2012 through 2023.

Number of South Carolina Residents Affected by Security Breaches by Industry January 2019 – December 2023

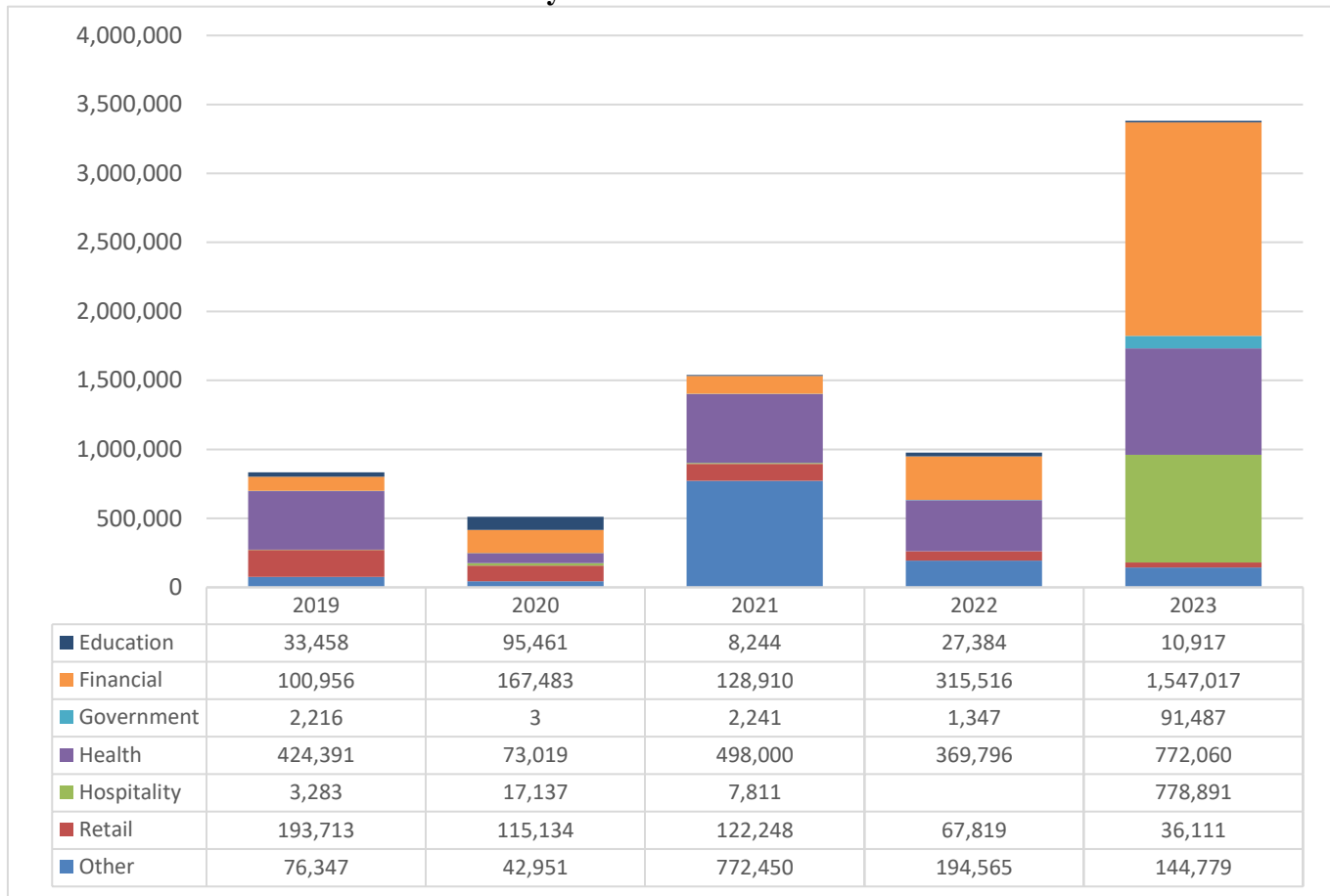


Figure 2

Over 7.2 million¹ South Carolina residents were affected by the 421 security breaches reported January 2019 through December 2023. For these years, 2023 represents the year with the largest number of South Carolina residents being affected by breaches with 3,381,262 in addition to the highest number of notices (138). The total number of residents affected by breaches for the remaining years included in this report are as follows: 976,427 (2022); 1,539,904 (2021); 511,188 (2020); 834,364 (2019).

For breaches reported during 2019–2023, the breaches impacting the largest number of residents were reported in 2023 by financial organizations (1,547,017), hospitality industry (778,891), healthcare organizations (772,060), and government (91,487). Healthcare organizations also reported the highest number of residents in 2022. The highest number reported for the other industries was by other (772,450 in 2021), retail (193,713 in 2019), and education (95,461 in 2020).

¹ Please be aware as you read the information provided that many companies and organizations were unable to report a specific number of consumers affected, even after a thorough investigation had been completed. In these instances, the number of consumers affected was recorded as “0.” Therefore, the totals provided reflect the minimum number of South Carolina residents potentially affected and the actual number is likely significantly higher.

**Total Number of Notices and Affected Residents per Industry
January 2019 – December 2023**

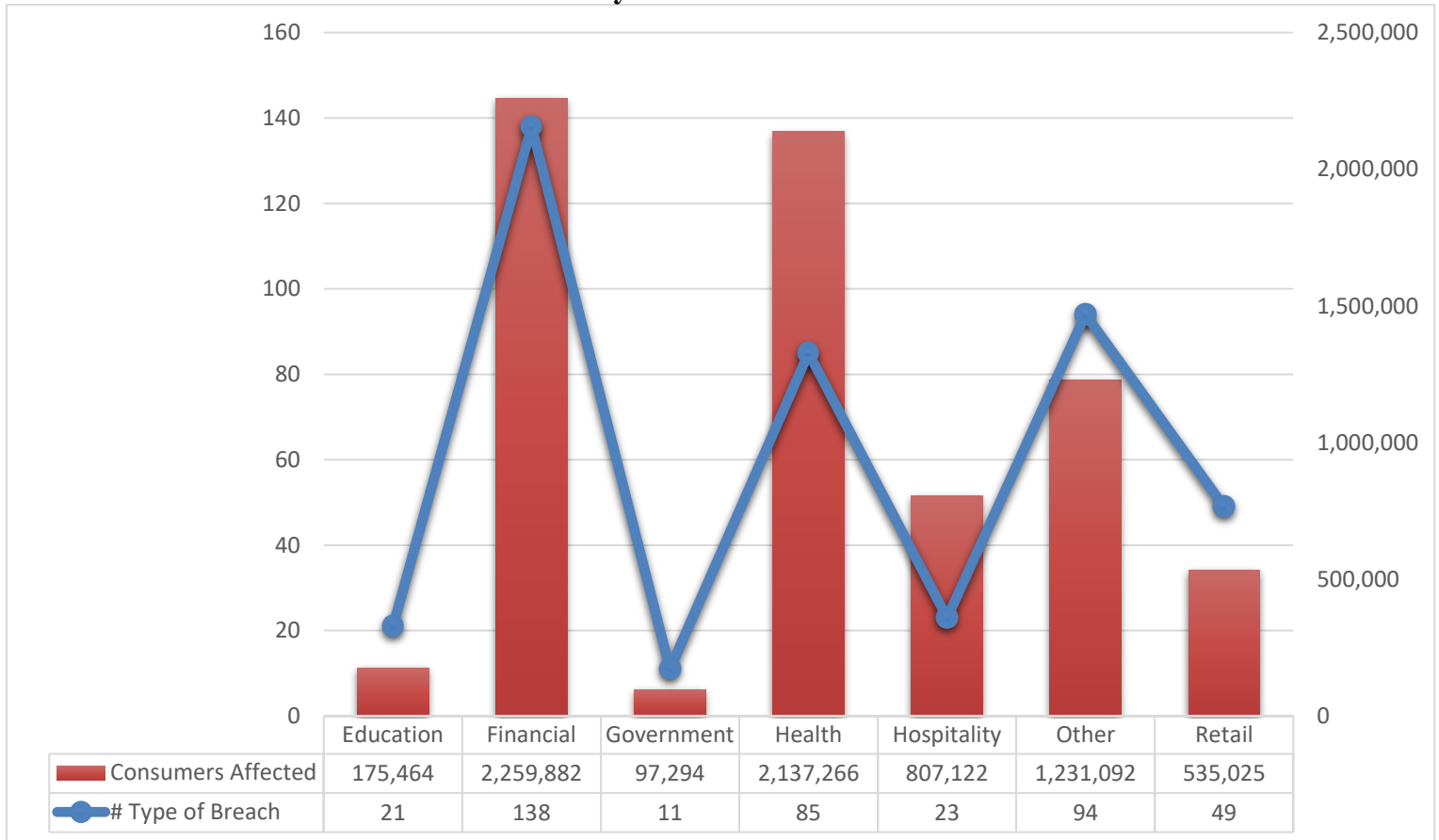


Figure 3

From January 2019 through December 2023, financial service providers reported one hundred thirty-eight security breaches affecting just over 2.25 million residents. The healthcare industry reported eighty-five security breaches that affected just over 2.1 million residents. The hospitality industry reported twenty-three breaches, which affected 807,122 residents. The retail industry reported forty-nine security breaches that affected nearly half a million residents. Education providers reported twenty-one security breaches affecting 175,464 residents. Governmental entities reported eleven security breaches affecting just over ninety-seven thousand South Carolina residents. Other industries falling outside these six main sectors filed ninety-four notices affecting just over 1.2 million consumers.

Types of Breaches January 2019 – December 2023

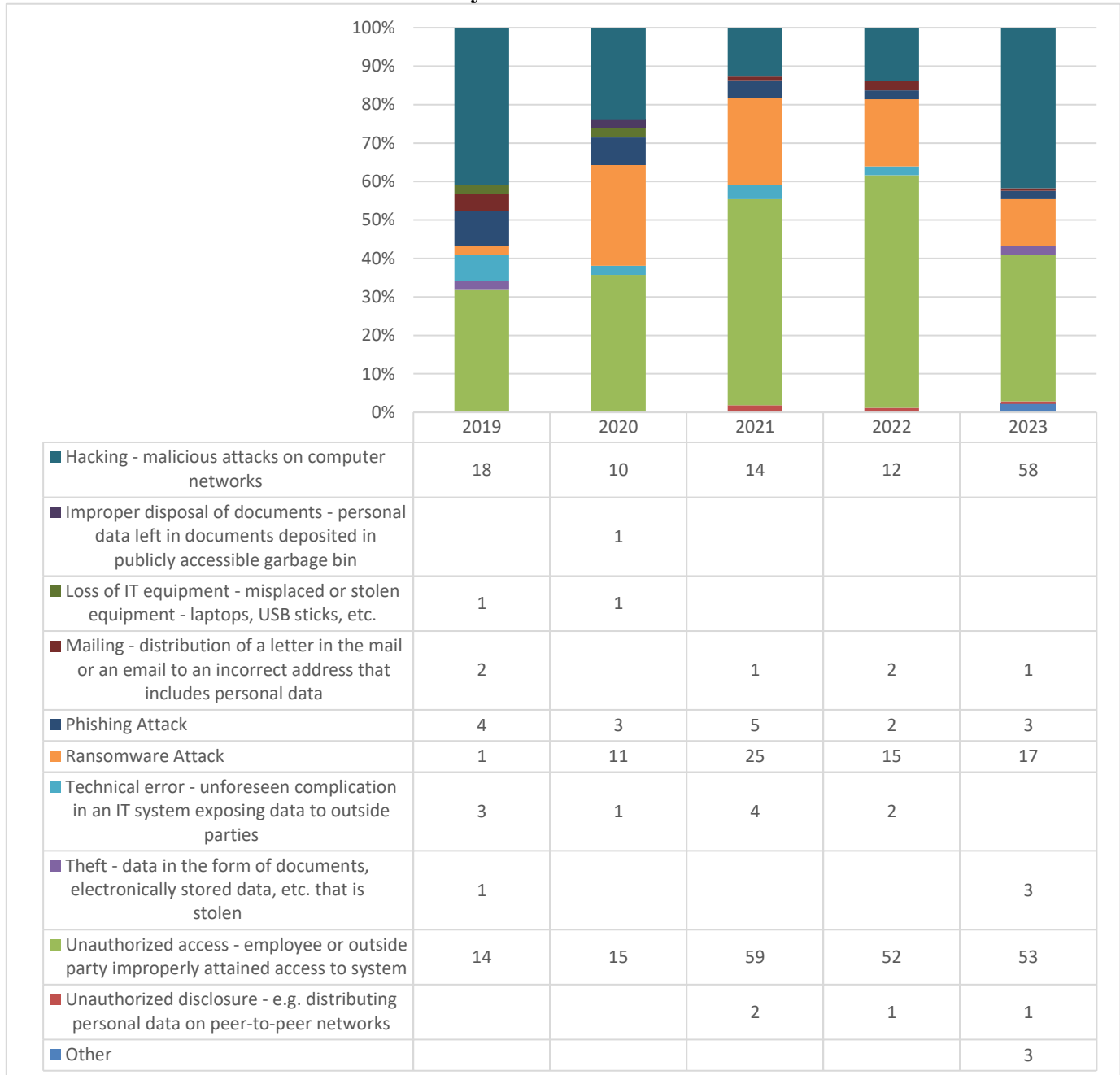


Figure 4

From 2019 to 2023, the most prevalent types of breaches have been unauthorized access (193), followed by hacking (112) and ransomware attacks (69). These three types of breaches account for 89% of the total number reported. The remaining 11% include seventeen due to phishing attacks; ten caused by an unforeseen technical error; six due to mailing errors; four due to theft; four caused by unauthorized disclosure; two due to a loss of IT equipment; one due to the improper disposal of documents; and three not falling within any of the other types listed.

In Depth Look at the Types of Breaches in 2023

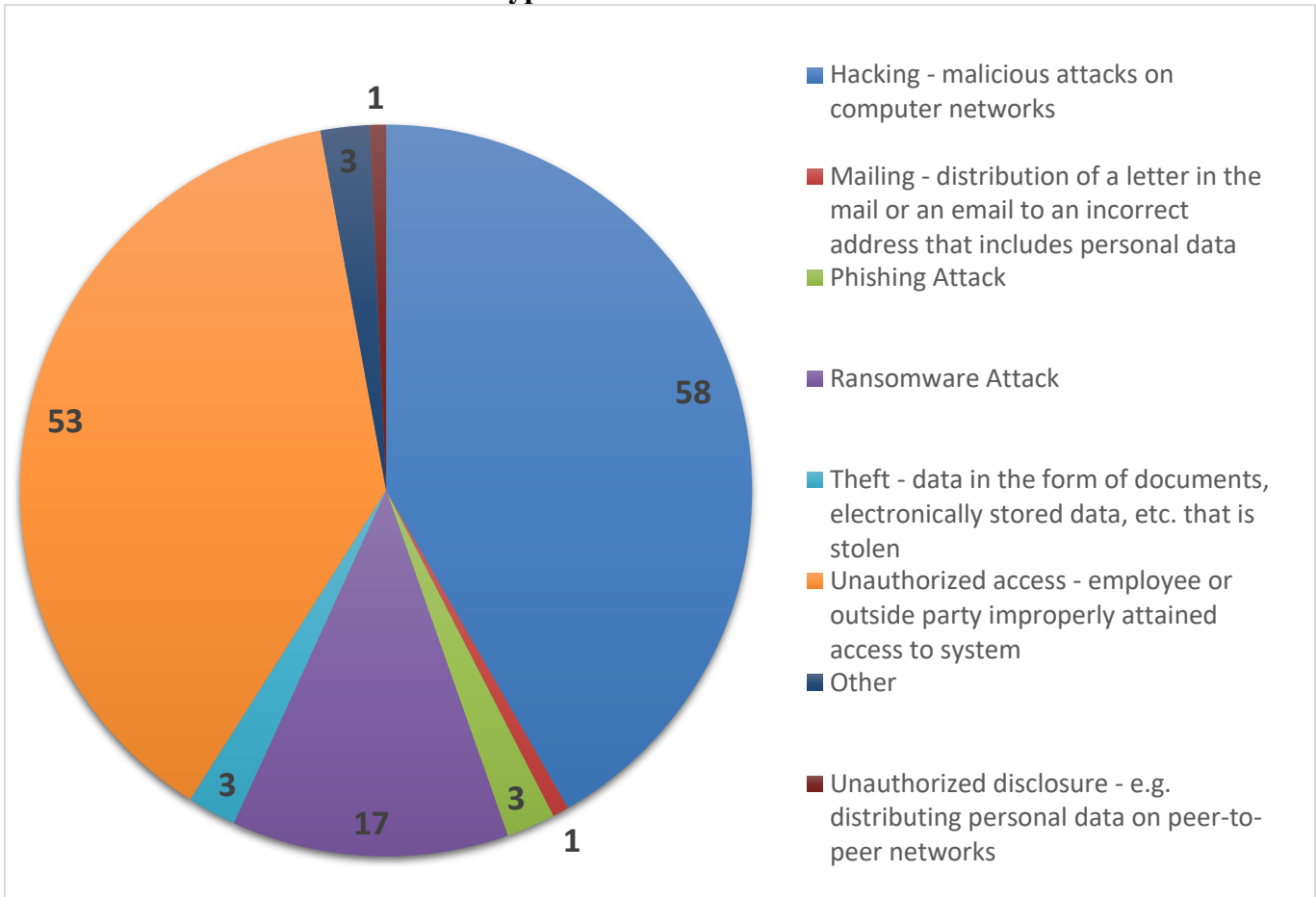


Figure 5

In 2023, SCDCA received fifty-eight reports of security breaches due to hacking, representing 42% of the total breaches reported for the year. Fifty-three security breach notices (38% of total) were due to unauthorized access. Seventeen breaches (12% of total) were due to ransomware attacks. The remaining 8% of the total breaches reported were three breaches due to theft; three breaches due to phishing attacks; one breach due to a distribution of a letter in the mail or an email to an incorrect address that includes personal data; one breach due to unauthorized disclosure, e.g., distributing personal data on peer-to-peer networks; and three not falling within any of the other types listed.

Most notably, the number of hacking – malicious attacks on computer networks significantly increased in 2023 (58), exceeding the combined total of the hacking breaches reported 2019–2022 (54). Furthermore, hacking accounted for more breaches than unauthorized access in 2023 for the first time since 2019.

Types of Data Breached January 2019 – December 2023

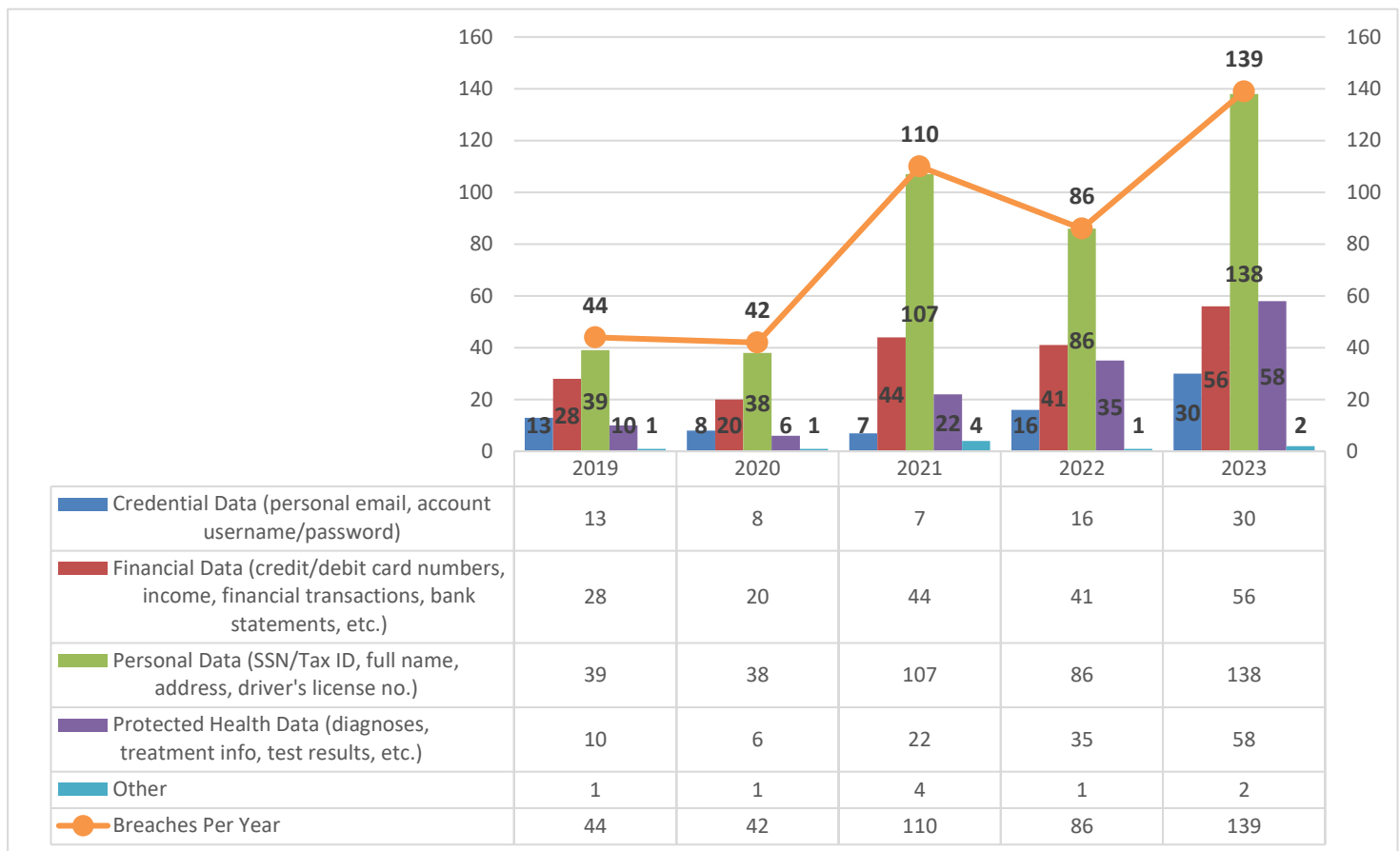


Figure 6

From 2019 to 2023, SCDCA received 421 reports of security breaches. Of those, 408 (97%) of reported breaches involved the exposure of protected personal data; 189 (44.9%) involved financial data; 131 (31.1%) indicated compromised protected health data; 74 (17.6%) implicated credential data; and nine (2.1%) involved other types of potentially sensitive information, such as location data and academic history.² Notably, for 2023, the percentage of breach reports indicating compromised protected health data continued the trend of increasing year over year: 14.3% in 2020; 20% in 2021; 40.7% in 2022; and 41.7% in 2023.

² SCDCA's methodology recognizes that multiple types of data can be breached within one security breach.

Remediation Steps Taken by Reporting Organizations January 2019 – December 2023

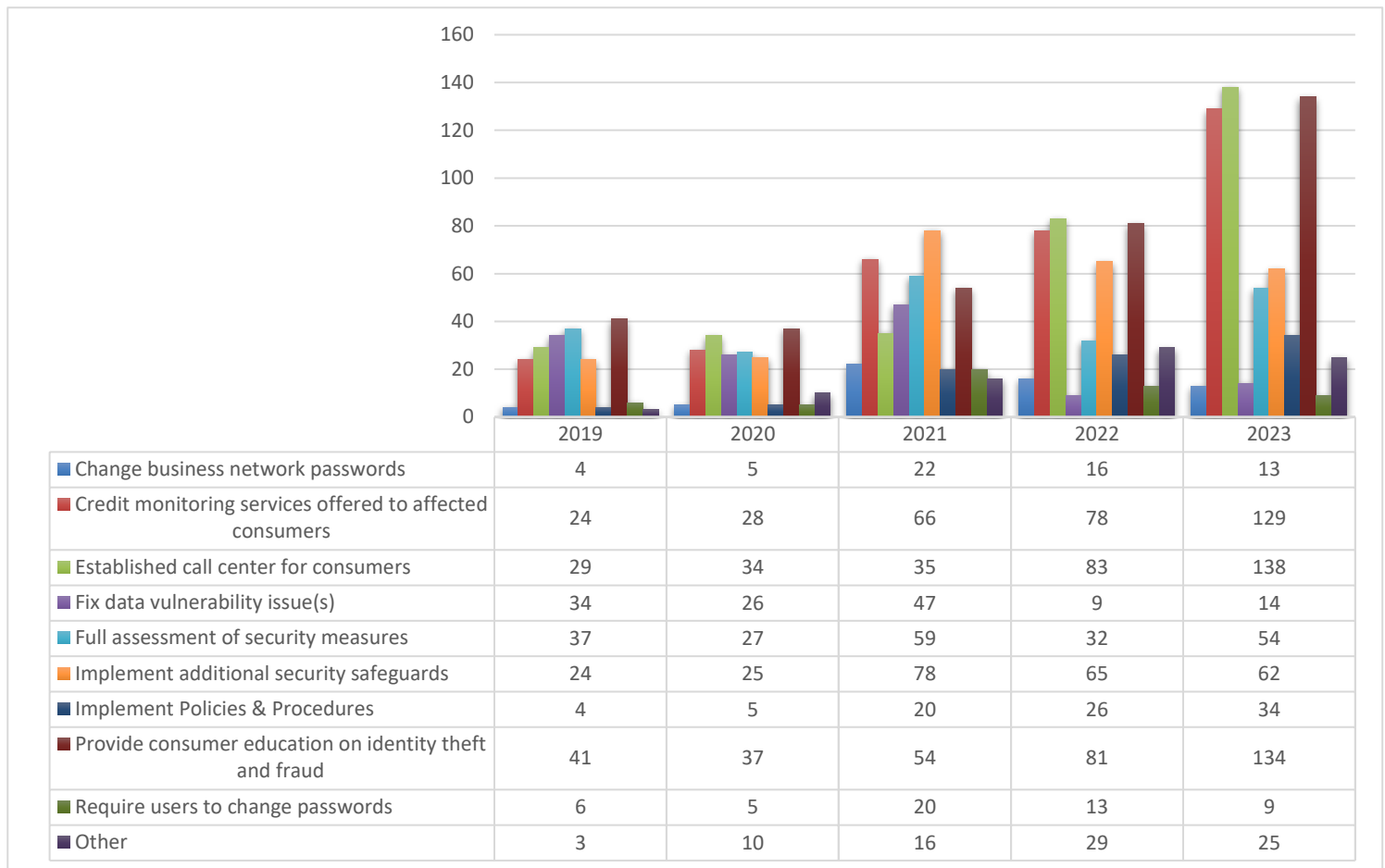


Figure 7

In 2017, SCDCA began capturing the remediation steps taken by the reporting organizations and completed a review of the steps taken in previously-reported breaches, as well.³ For the 421 breaches reported 2019–2023, 82.4% provided consumer education on identity theft and fraud; 77.2% offered free credit monitoring services to affected consumers; 75.8% established a dedicated call center for affected consumers; 60.3% implemented additional security safeguards; 49.6% initiated a full assessment of their security measures; 30.9% fixed data vulnerability issues; 21.1% implemented policies and procedures related to protecting sensitive data; 14.3% changed their business network passwords; 12.6% required users to change their passwords; and 19.7% took remediation steps outside of the other nine categories. Some examples of other remediation measures taken include: the implementation of two-factor authentication, employee training, termination of third-party contracts, and the addition of encryption software. In 2023, for the second consecutive year, the top three remediations measures were establishing dedicated call centers for consumers (99.3%), providing consumer education (96.4%), and offering credit monitoring services (92.8%).

³ SCDCA's methodology tracks multiple remediation steps taken by an organization in response to a security breach.

For those South Carolina residents who may have been affected by a security breach or would like more information about protecting their personal information, visit consumer.sc.gov and click the “Identity Theft Unit” button or call us toll-free at 1-800-922-1594.

For details on what action to take in resolving specific identity theft problems, consumers can contact SCDCA’s Identity Theft Unit at the number above or fill out an Identity Theft Intake Form online.

