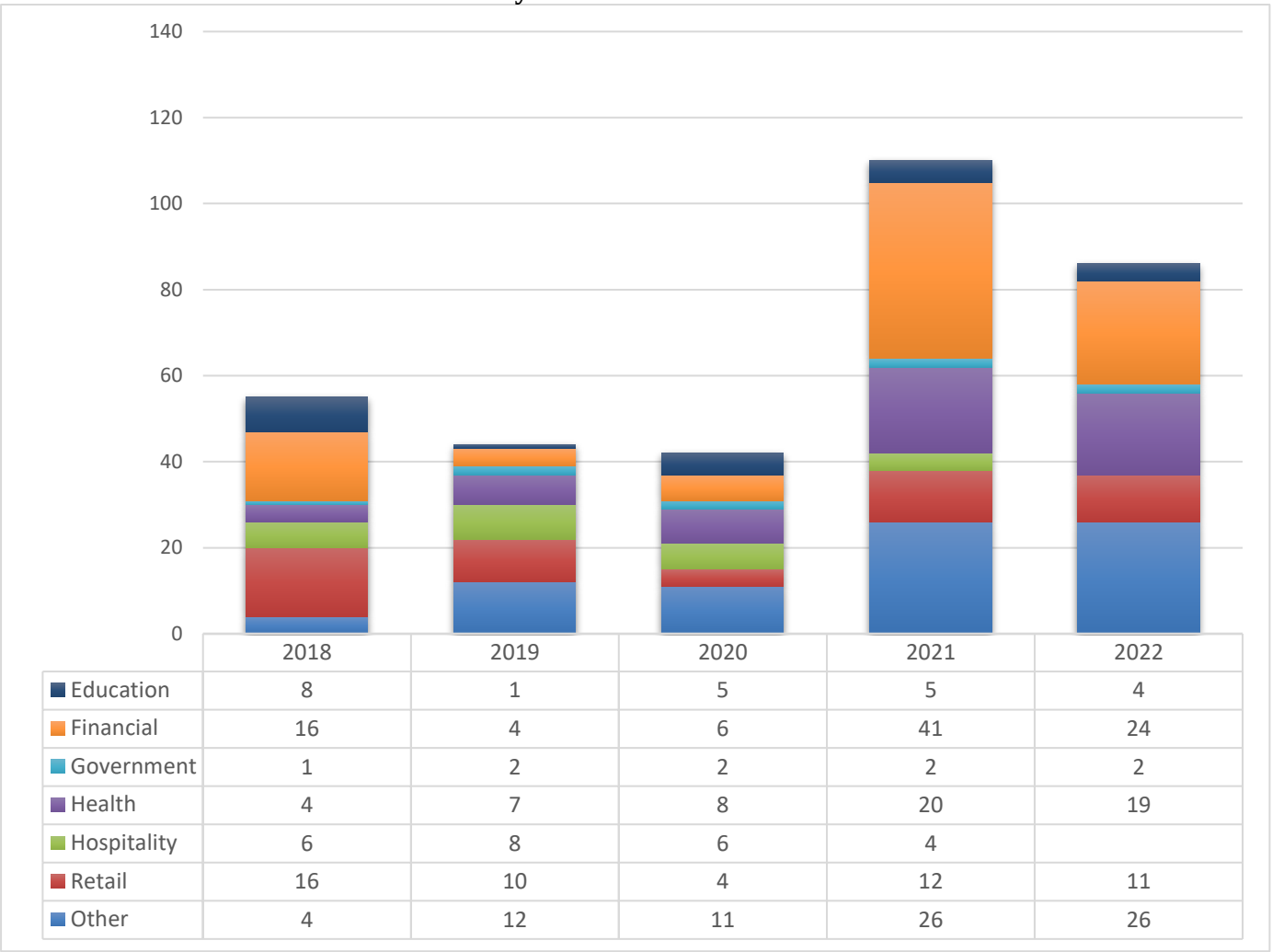
Security Breach Notice Report

An overview of the security breach notices received by SCDCA since 2018 as well as a detailed analysis of the security breach notices received in 2022.

2023

Number of Security Breach Notices Received by Industry
January 2018 – December 2022



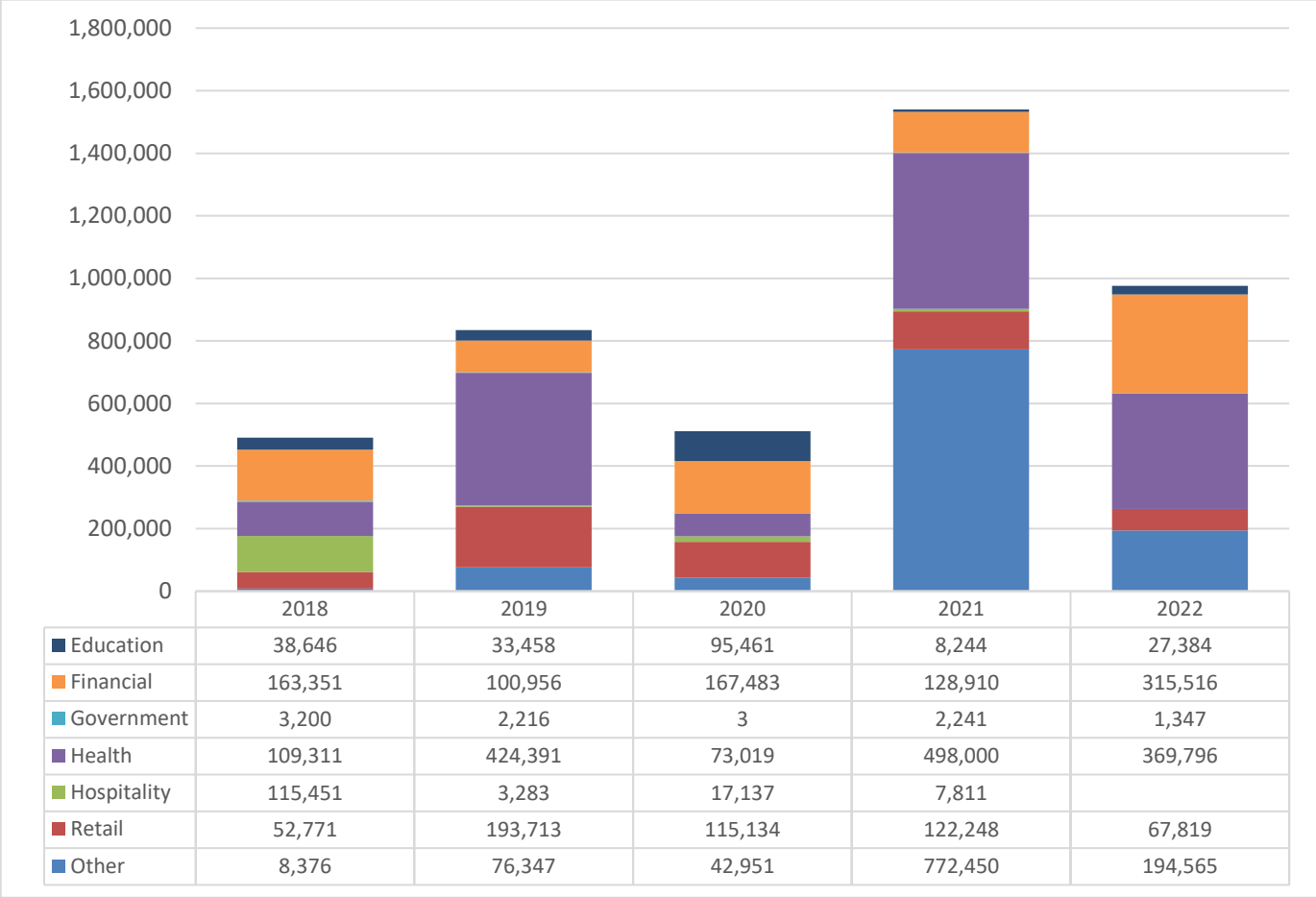
	2018	2019	2020	2021	2022
Education	8	1	5	5	4
Financial	16	4	6	41	24
Government	1	2	2	2	2
Health	4	7	8	20	19
Hospitality	6	8	6	4	
Retail	16	10	4	12	11
Other	4	12	11	26	26

Figure 1

From January 2018 through December 2022, SCDCA received **337** breach notices. A total of ninety-one (91) from financial service providers, fifty-eight (58) from healthcare organizations, fifty-three (53) breaches were reported by the retail industry, twenty-four (24) from the hospitality industry, twenty-three (23) from education providers, and nine (9) from governmental entities. SCDCA also received seventy-nine (79) reports of breaches from organizations outside these six main categories.

SCDCA received 86 notices in 2022, down from the most notices reported in 2021 (110). Compared to 2021 and 2022, the number of notices received were relatively stable in years 2018 (55), 2019 (44), and 2020 (42).

Number of South Carolina Residents Affected by Security Breaches by Industry
January 2018 – December 2022



	2018	2019	2020	2021	2022
Education	38,646	33,458	95,461	8,244	27,384
Financial	163,351	100,956	167,483	128,910	315,516
Government	3,200	2,216	3	2,241	1,347
Health	109,311	424,391	73,019	498,000	369,796
Hospitality	115,451	3,283	17,137	7,811	
Retail	52,771	193,713	115,134	122,248	67,819
Other	8,376	76,347	42,951	772,450	194,565

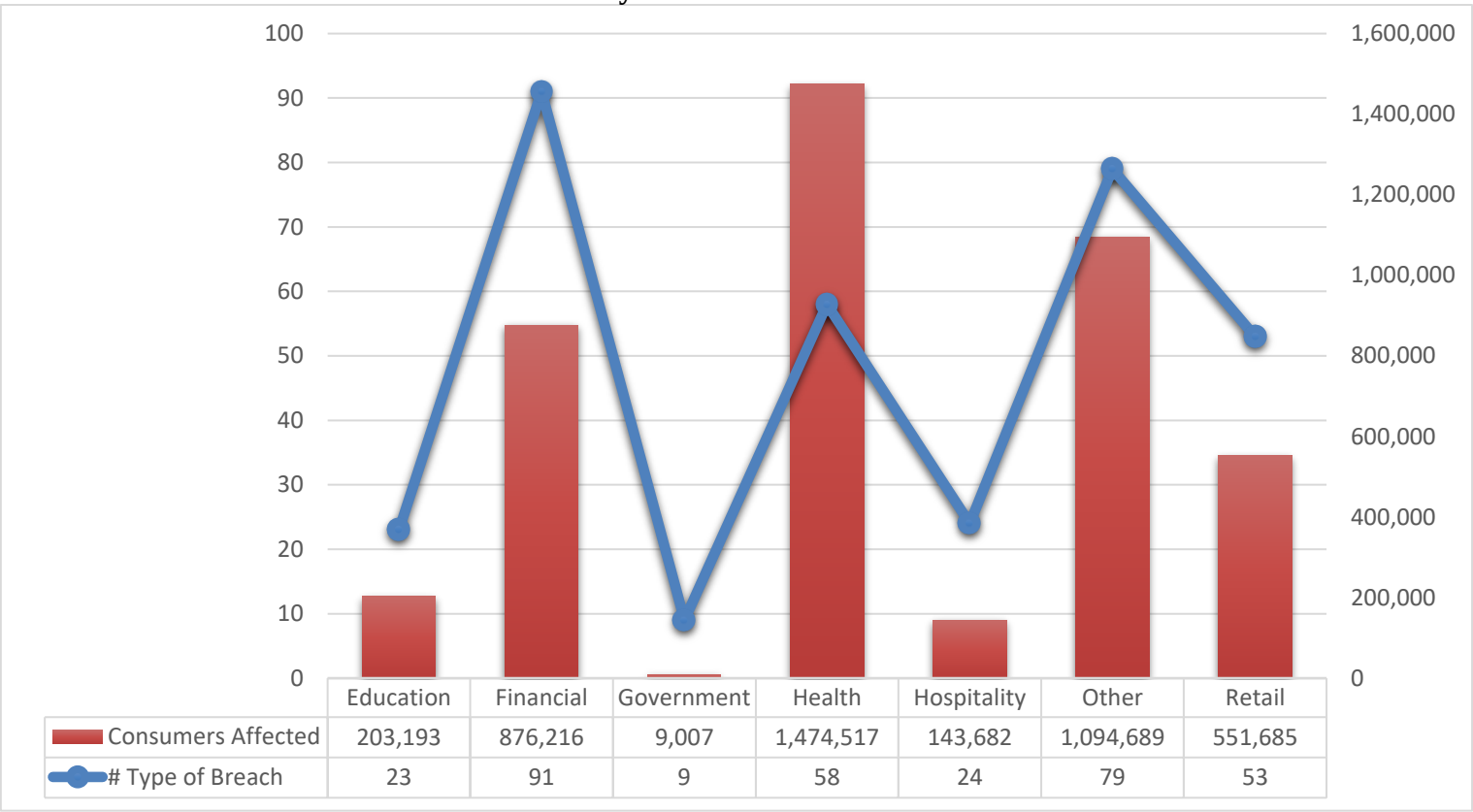
Figure 2

Over 4 million[1] South Carolina residents were affected by the 337 security breaches reported January 2018 through December 2022. The total number of residents affected in 2022 was 976,427, down from 2021 (1,539,904). The total number of residents affected by breaches for the remaining years included in this report are as follows: 511,188 (2020); 834,364 (2019); 491,106 (2018).

For breaches reported during 2018–2022, the breaches from organizations outside the six main categories impacted the largest number of South Carolina residents at 772,450 in 2021. Healthcare organizations reported breaches affecting the most residents for the years 2022 (369,796) and 2019 (424,391). Reported breaches involving financial organizations affected the most residents in 2020 (167,483) and 2018 (163,351).

[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 2018 – December 2022

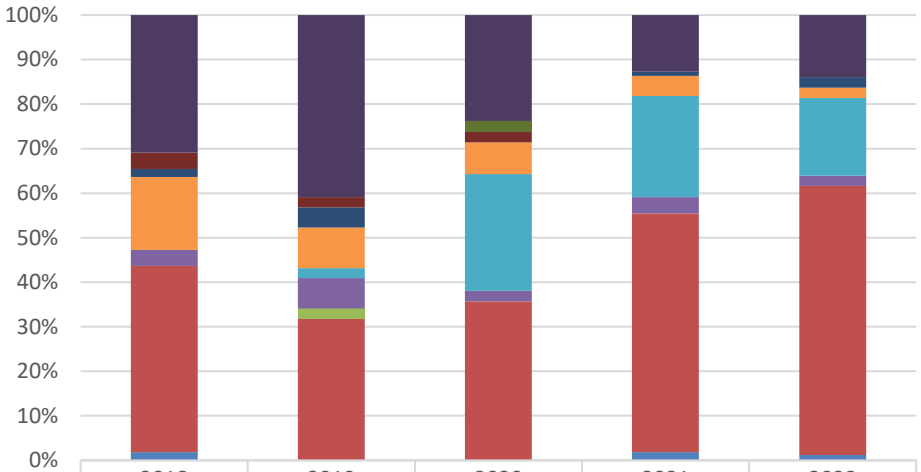


	Education	Financial	Government	Health	Hospitality	Other	Retail
Consumers Affected	203,193	876,216	9,007	1,474,517	143,682	1,094,689	551,685
# Type of Breach	23	91	9	58	24	79	53

Figure 3

From January 2018 through December 2022, education providers reported twenty-three security breaches affecting 203,193 residents. Financial service providers reported ninety-one security breaches affecting 876,216 residents. Governmental entities reported nine security breaches affecting just over nine thousand South Carolina residents. The healthcare industry reported fifty-eight security breaches that affected just under 1.5 million residents. The hospitality industry reported twenty-four breaches, which affected 143,682 residents. The retail industry reported fifty-three security breaches that affected over half a million residents. Other industries falling outside these six main sectors filed seventy-nine notices affecting nearly 1.1 million consumers.

Types of Breaches
January 2018 – December 2022



	2018	2019	2020	2021	2022
Hacking - malicious attacks on computer networks	17	18	10	14	12
Improper disposal of documents - personal data left in documents deposited in publicly accessible garbage bin			1		
Loss of IT equipment - misplaced or stolen equipment - laptops, USB sticks, etc.	2	1	1		
Mailing - distribution of a letter in the mail or an email to an incorrect address that includes personal data	1	2		1	2
Phishing Attack	9	4	3	5	2
Ransomware Attack		1	11	25	15
Technical error - unforeseen complication in an IT system exposing data to outside parties	2	3	1	4	2
Theft - data in the form of documents, electronically stored data, etc. that is stolen		1			
Unauthorized access - employee or outside party improperly attained access to system	23	14	15	59	52
Unauthorized disclosure - e.g. distributing personal data on peer-to-peer networks	1			2	1

Figure 4

From 2018 to 2022, the most prevalent types of breaches have been unauthorized access (163), followed by hacking (71) and ransomware attacks (52). These three types of breaches account for 85% of the total number reported. The remaining 15% include twenty-three due to phishing attacks; twelve caused by an unforeseen technical error; six due to mailing errors; four due to a loss of IT equipment; four caused by unauthorized disclosure; one due to theft; and one due to the improper disposal of documents.

In Depth Look at the Types of Breaches in 2022

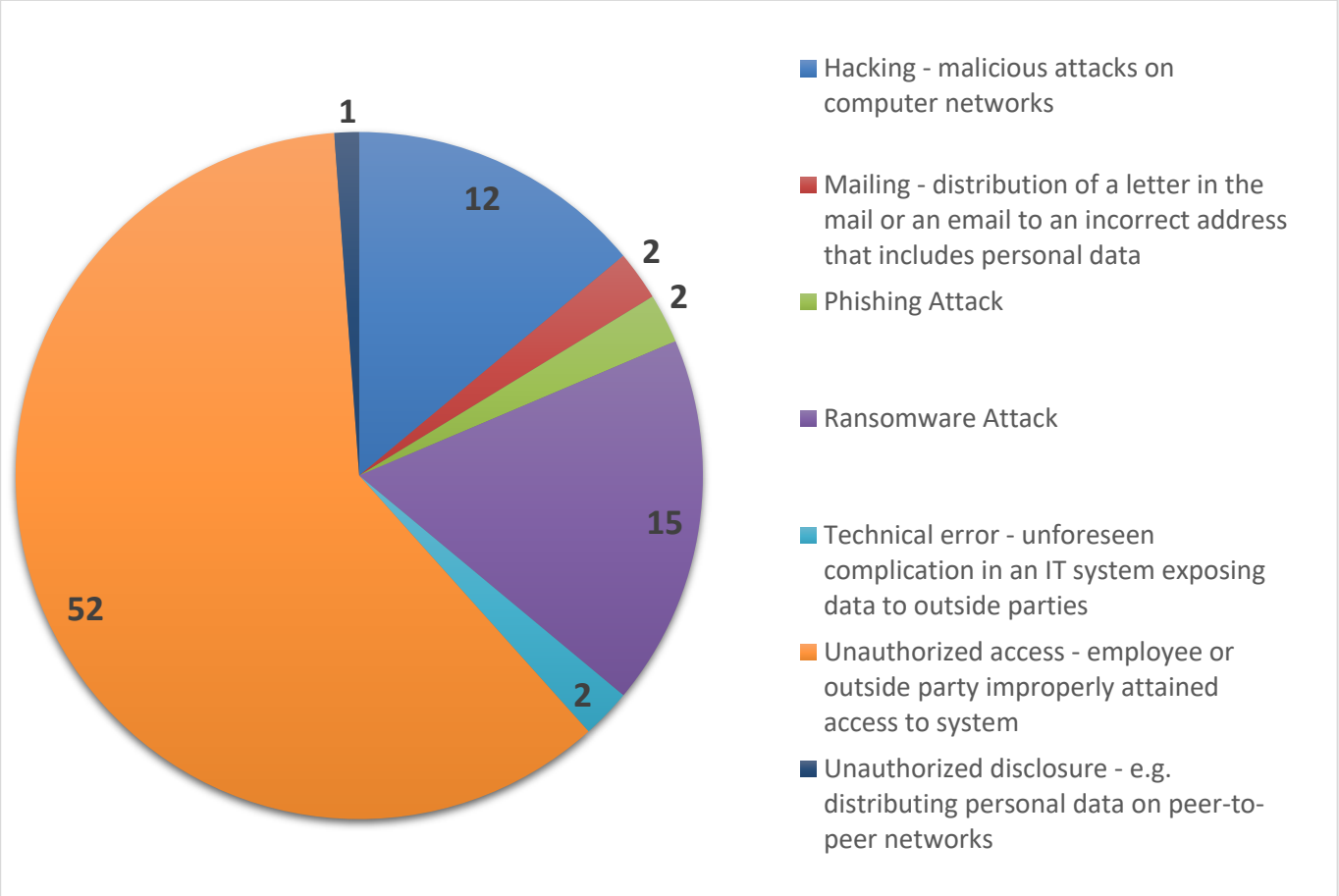
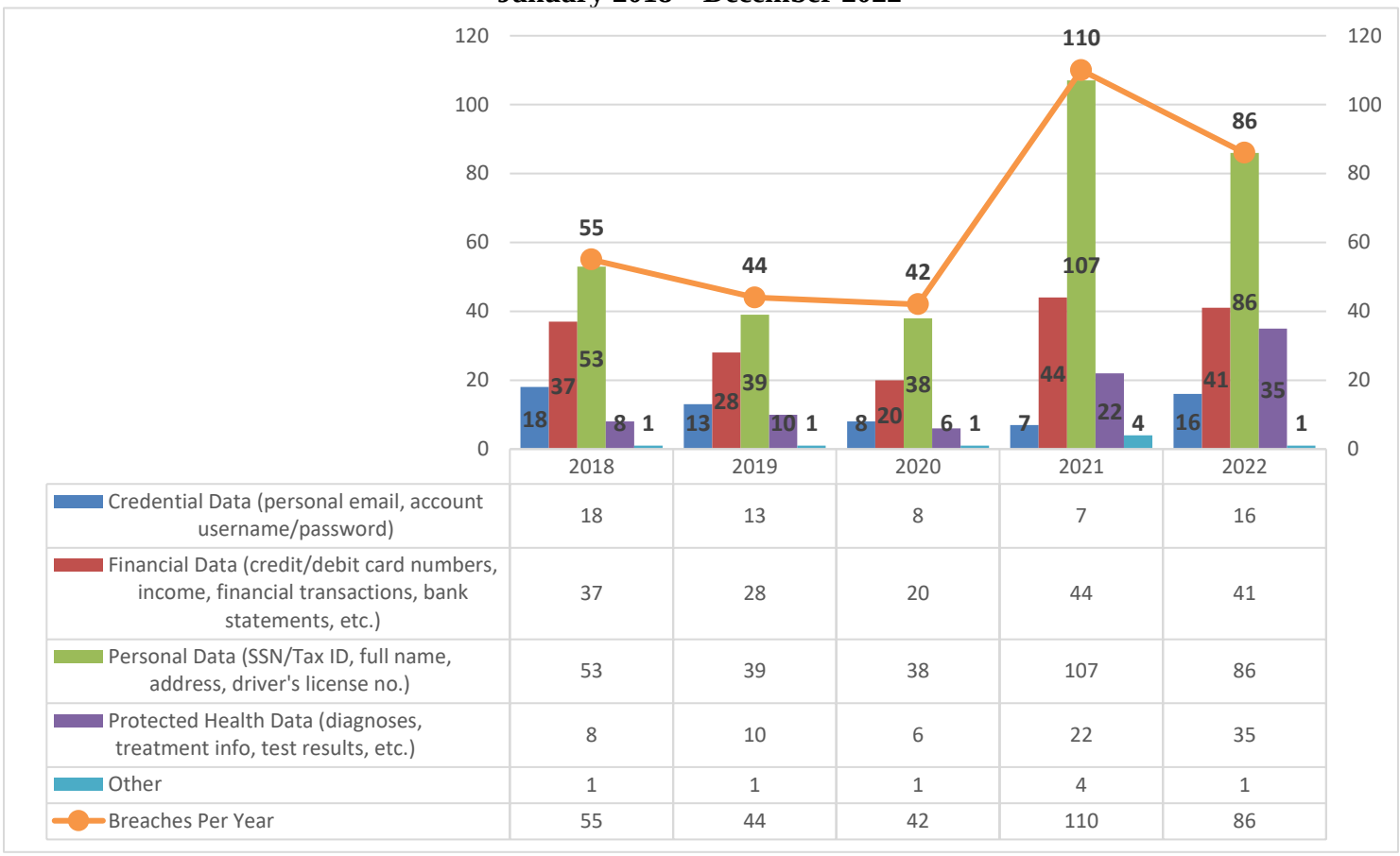


Figure 5

In 2022, SCDCA received fifty-two security breach notices due to unauthorized access, representing more than 60% of the total breaches reported for the year. Fifteen breaches (17% of total) were due to ransomware attacks. Twelve reports of security breaches (14% of total) were due to hacking. The remaining 9% of the total breaches reported were two breaches due to a technical error; two security breaches due to phishing attacks; two security breaches due to a distribution of a letter in the mail or an email to an incorrect address that includes personal data; and one security breach report due to unauthorized disclosure, e.g., distributing personal data on peer-to-peer networks.

Types of Data Breached
January 2018 – December 2022



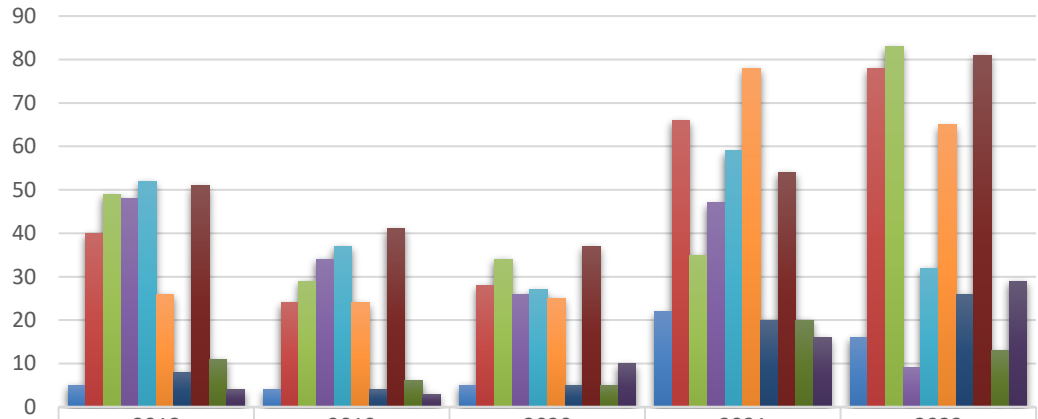
	2018	2019	2020	2021	2022
Credential Data (personal email, account username/password)	18	13	8	7	16
Financial Data (credit/debit card numbers, income, financial transactions, bank statements, etc.)	37	28	20	44	41
Personal Data (SSN/Tax ID, full name, address, driver's license no.)	53	39	38	107	86
Protected Health Data (diagnoses, treatment info, test results, etc.)	8	10	6	22	35
Other	1	1	1	4	1
Breaches Per Year	55	44	42	110	86

Figure 6

From 2018 to 2022, SCDCA received 337 reports of security breaches. Of the 337 reports received, 323 (95.8%) implicated personal data; 170 (50.4%) indicated a breach of financial data; 81 (24%) indicated compromised protected health data; 62 (18.4%) implicated credential data; and eight (2.4%) indicated a breach of other types of potentially sensitive information, such as location data and academic history.[2] For the second consecutive year, more breaches affected protected health data (40.6%) than credential data (18.6%).

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

Remediation Steps Taken by Reporting Organizations
January 2018 – December 2022



	2018	2019	2020	2021	2022
Change business network passwords	5	4	5	22	16
Credit monitoring services offered to affected consumers	40	24	28	66	78
Established call center for consumers	49	29	34	35	83
Fix data vulnerability issue(s)	48	34	26	47	9
Full assessment of security measures	52	37	27	59	32
Implement additional security safeguards	26	24	25	78	65
Implement Policies & Procedures	8	4	5	20	26
Provide consumer education on identity theft and fraud	51	41	37	54	81
Require users to change passwords	11	6	5	20	13
Other	4	3	10	16	29

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 beaches, as well.[3] For the 337 breaches reported 2018–2022, 78.3% provided consumer education on identity theft and fraud; 70% offered free credit monitoring services to affected consumers; 68.2% established a dedicated call center for affected consumers; 64.7% implemented additional security safeguards; 16.3% required users to change their passwords; 61.4% organizations initiated a full assessment of their security measures; 48.7% fixed data vulnerability issues; 18.7% implemented policies and procedures related to protecting sensitive data; 15.4% changed their business network passwords; and 18.4% took remediation steps outside of the other nine categories. Some examples of other remediation measures taken include implementation of two-factor authentication, employee training, termination of third-party contracts, and addition of encryption software. One of the most significant changes in 2022 is the increase in number of breaches where organizations established dedicated call centers for consumers (96.5% in 2022) from the previous 5-year average of 55.6%. Also in 2022, 94% provided consumer education and 90.6% offered credit monitoring services.

[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.

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS