



Security Breach Notice Report

An overview of the security breach notices received by SCDC from 2020 through 2024 as well as a detailed analysis of the security breach notices received in 2024.

2025

INTRODUCTION

To aid in combating identity theft, South Carolina passed the Financial Identity Fraud and Identity Theft Protection Act (“FIFITPA”) in 2008. Among other things, FIFITPA imposes security breach notification requirements on private business and public bodies. If a business sends notice of a security breach to 1,000 or more South Carolina residents at one time, the business must also notify the Department and the national credit reporting agencies. When a business is required to notify the Department of a breach, the notice should include all of the following:

1. Date of the breach;
2. Date business became aware of the breach;
3. Date notice was/will be sent to affected consumers;
4. Method of consumer notification (i.e., direct mail, electronic mail, etc.)
5. Number of affected South Carolina consumers;
6. Content of the consumer notice (i.e., copy of the letter sent to consumers); and
7. Action taken to avoid future breaches.

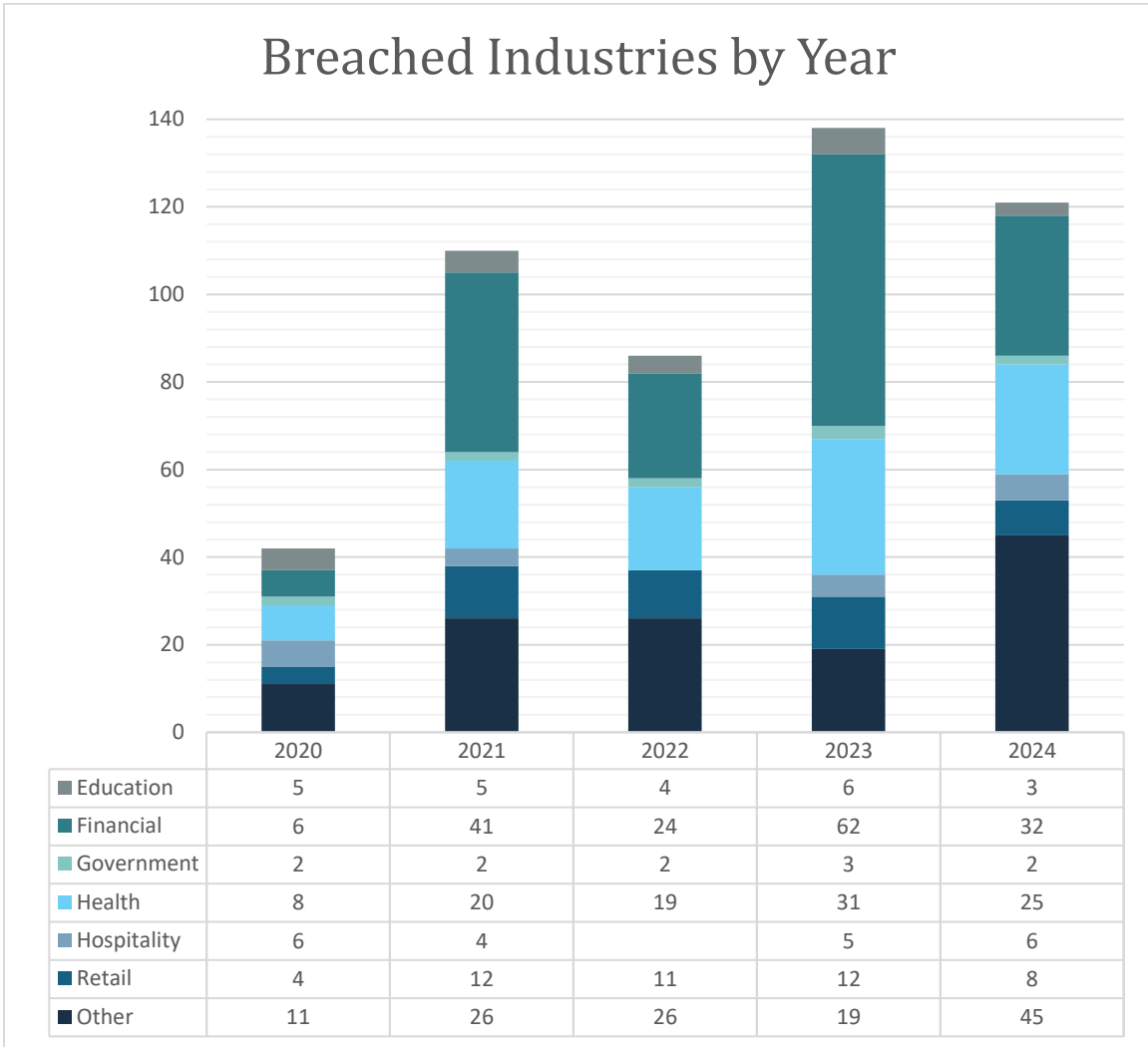
Breach notifications should be sent to the Department's Legal Division, P.O. Box 5757, Columbia, SC 29250 or emailed to scdca@scconsumer.gov.

For more information on the applicable laws in South Carolina, refer to the [Identity Theft & The Law: A Guide for Business and Government](#).

If you are a consumer who has been affected by a security breach and would like more information on how to keep your personal information safe, please see our [ID Theft](#) page for additional resources.

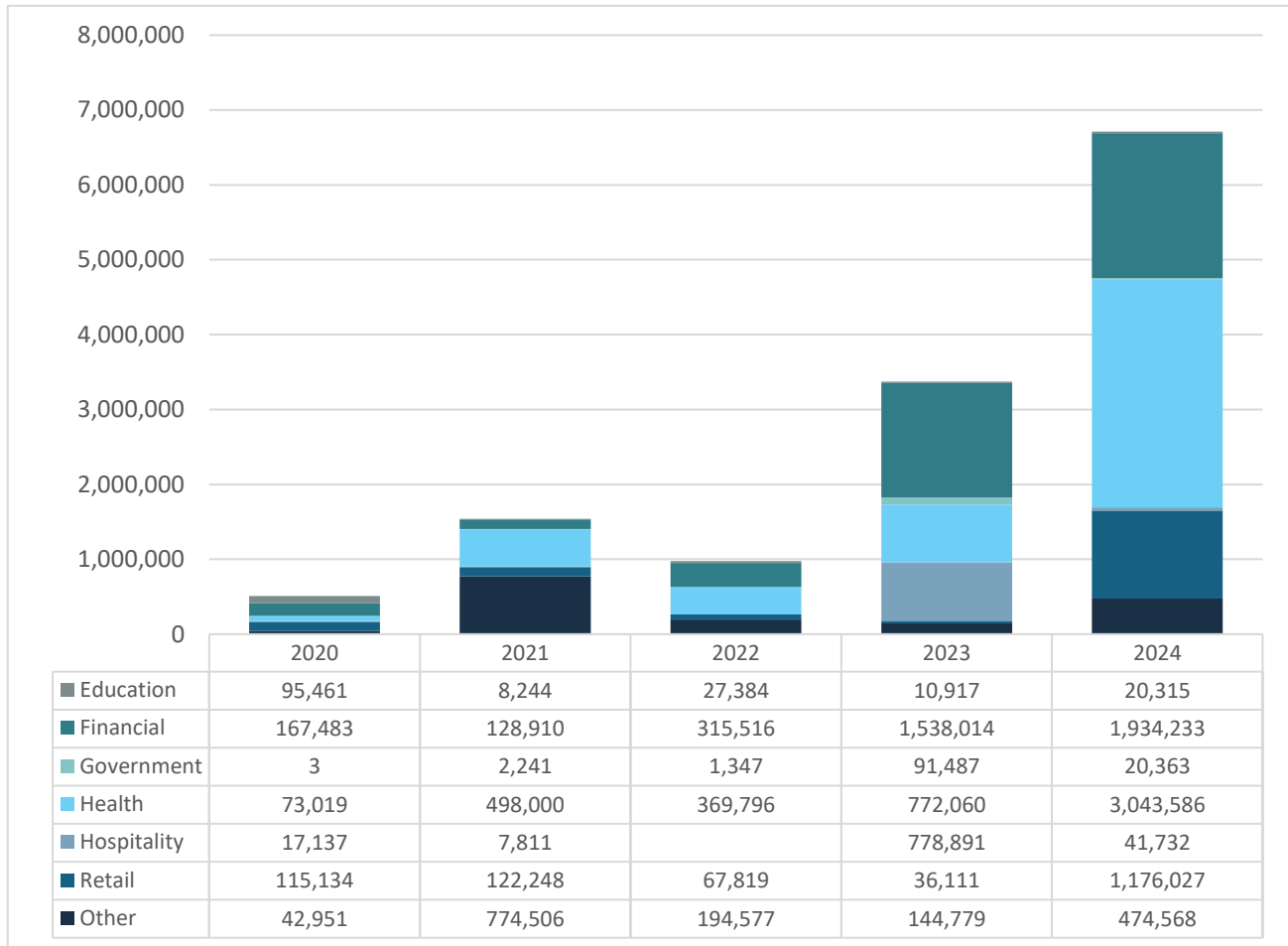
This report includes data received from businesses and government agencies that experienced a breach affecting South Carolina residents from 2020 through 2024. To view breach notices received by the Department, see our [Security Breach Notices](#) page.

**Number of Security Breach Notices Received by Industry
2020 – 2024**



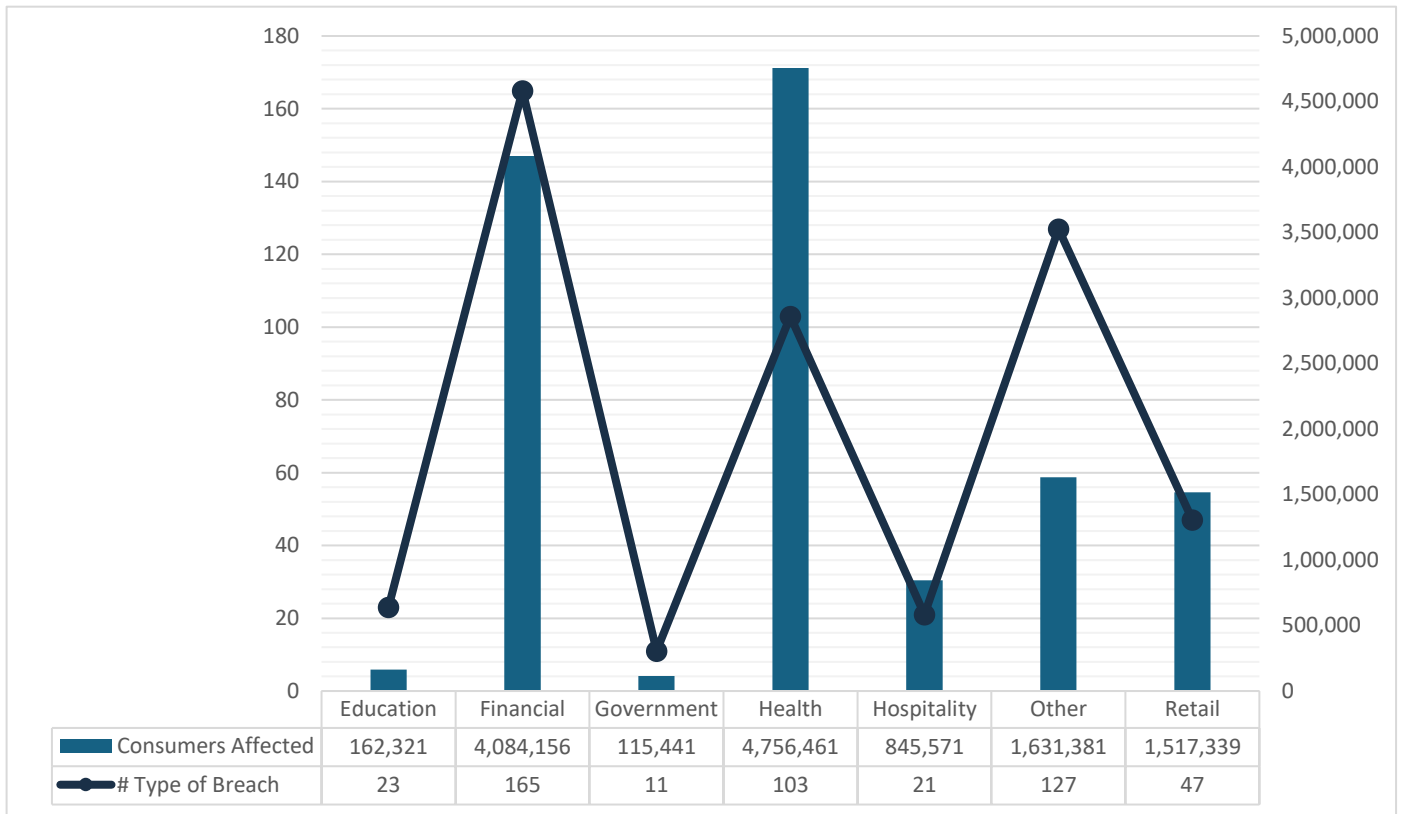
From 2020 to 2024, 497 businesses reported breaches to the South Carolina Department of Consumer Affairs (SCDCA). SCDCA received 42 notices in 2020. In 2021, 110 notices were received. In 2022, 86 notices were reported. In 2023, 138 notices were received. In 2024, 121 notices were received.

**Number of South Carolina Residents Affected by Security Breaches by Industry
2020 – 2024**



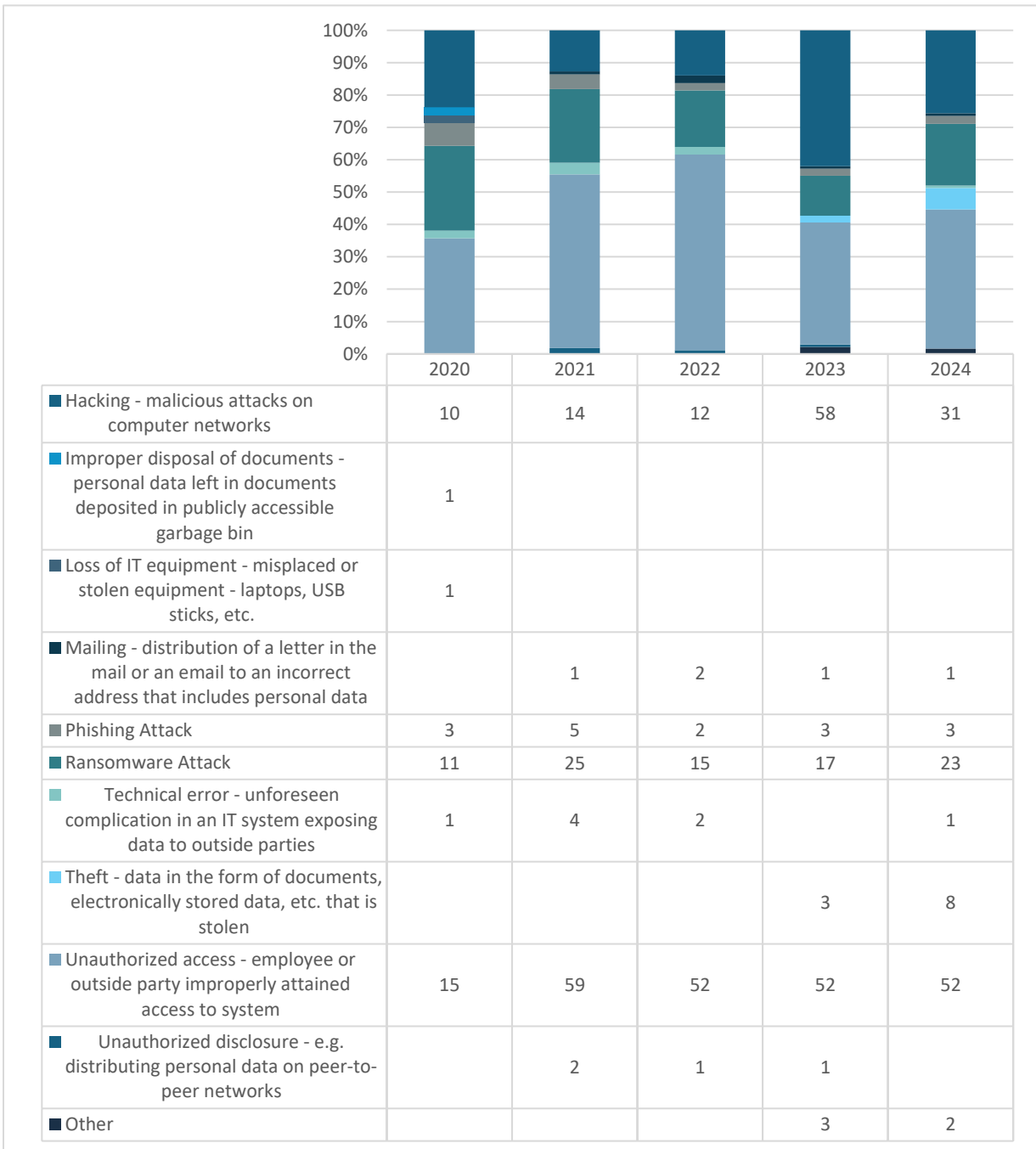
In 2024, breaches reported to SCDCA affected 6,710, 824 South Carolina consumers. Please be aware as you read the information provided that many companies and organizations were unable to report a specific number of consumers affected, even after a thorough investigation had been completed. In these 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
2020 – 2024**



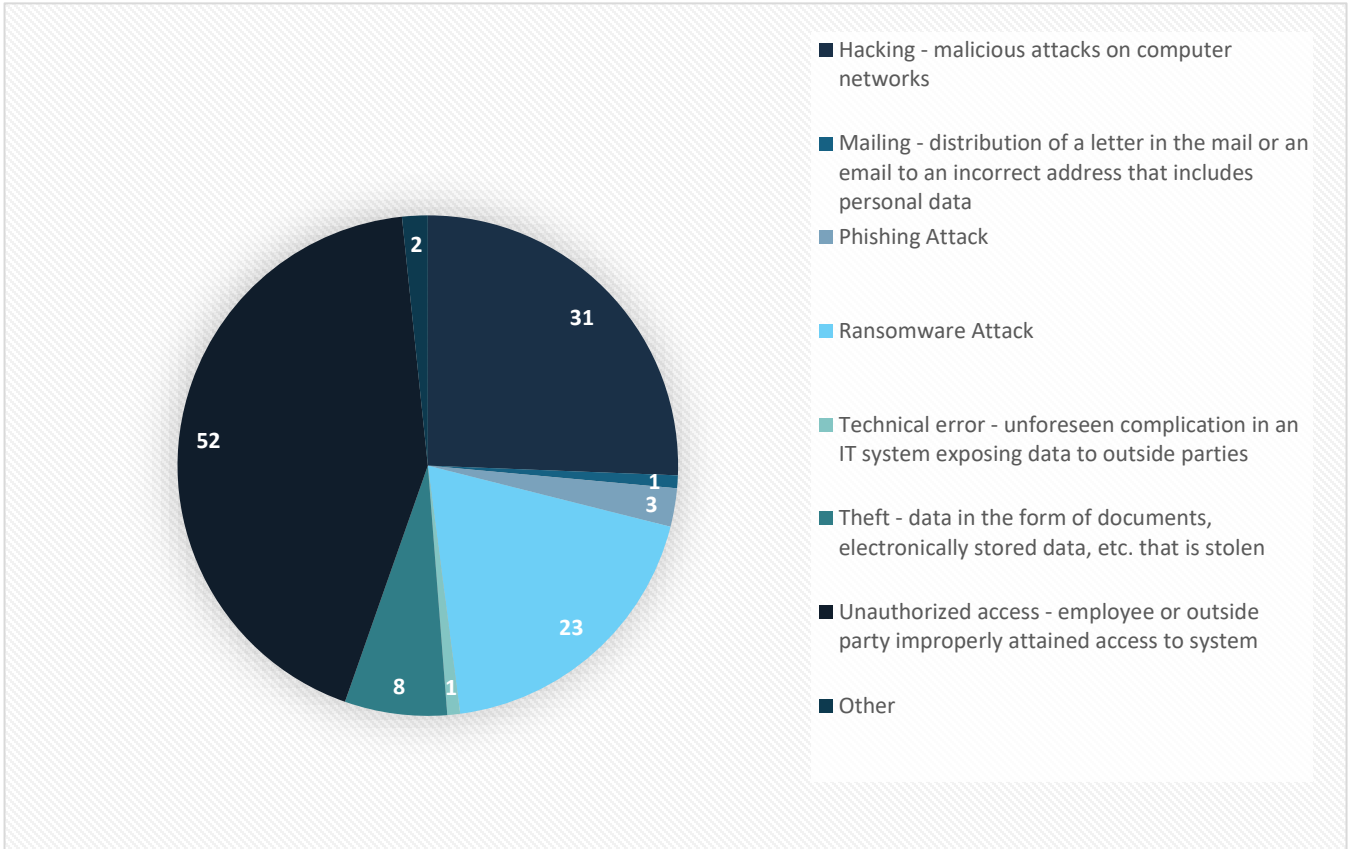
From 2020 through 2024, financial service providers reported one hundred sixty-five security breaches affecting just over 4.08 million residents. The healthcare industry reported one hundred and three security breaches that affected just over 4.75 million residents. The retail industry reported forty-seven security breaches that affected more than 1.51 million residents. Education providers reported twenty-three security breaches affecting 162,321 residents. The hospitality industry reported twenty-one breaches, which affected 845,571 residents. Governmental entities reported eleven security breaches affecting 115,441 South Carolina residents. Other industries falling outside these six main sectors filed one hundred twenty-seven notices affecting just over 1.63 million residents.

Types of Breaches 2020 – 2024



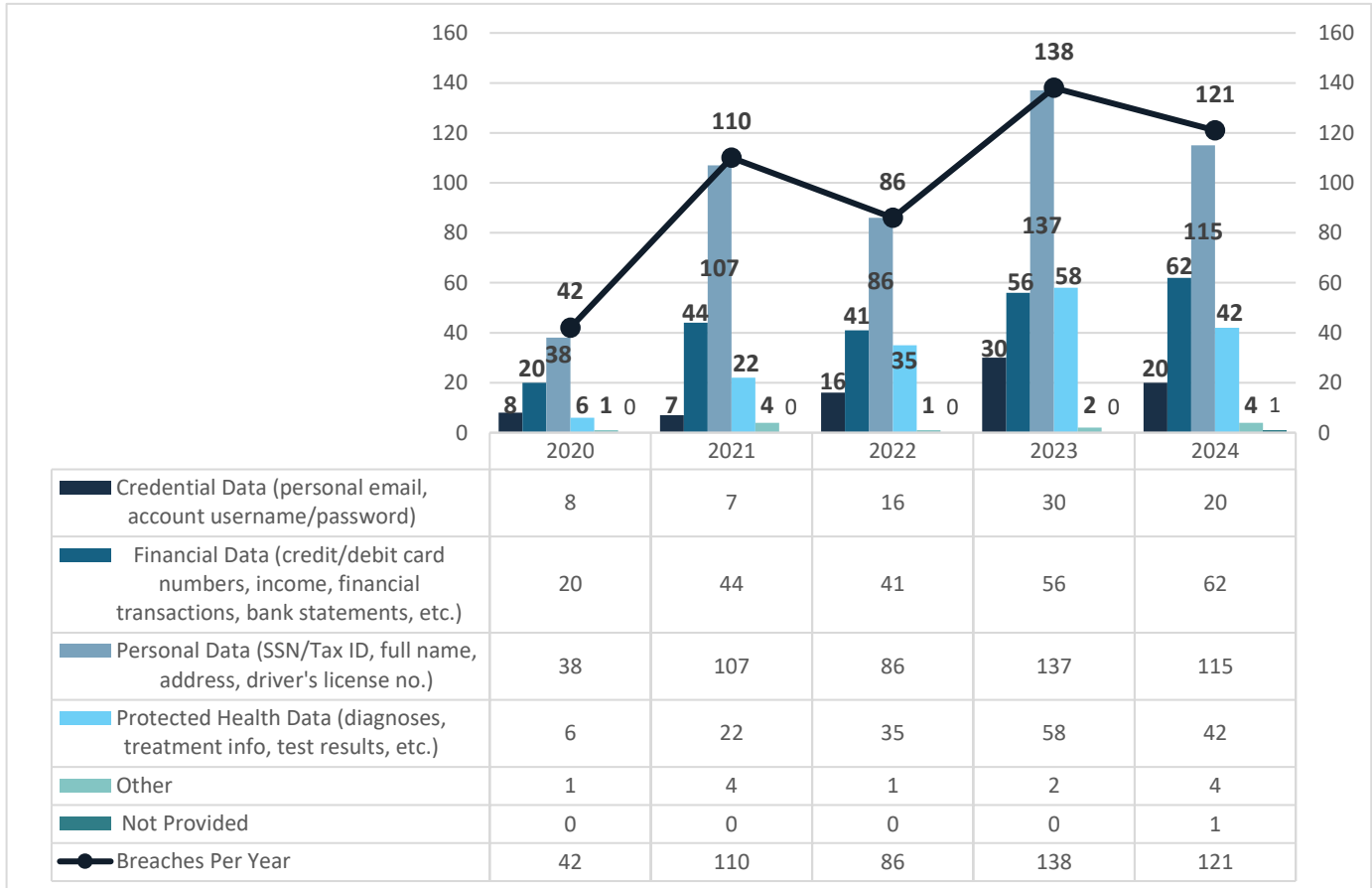
From 2020 to 2024, the most prevalent types of breaches have been unauthorized access (230), followed by hacking (125) and ransomware attacks (91).

In Depth Look at the Types of Breaches in 2024



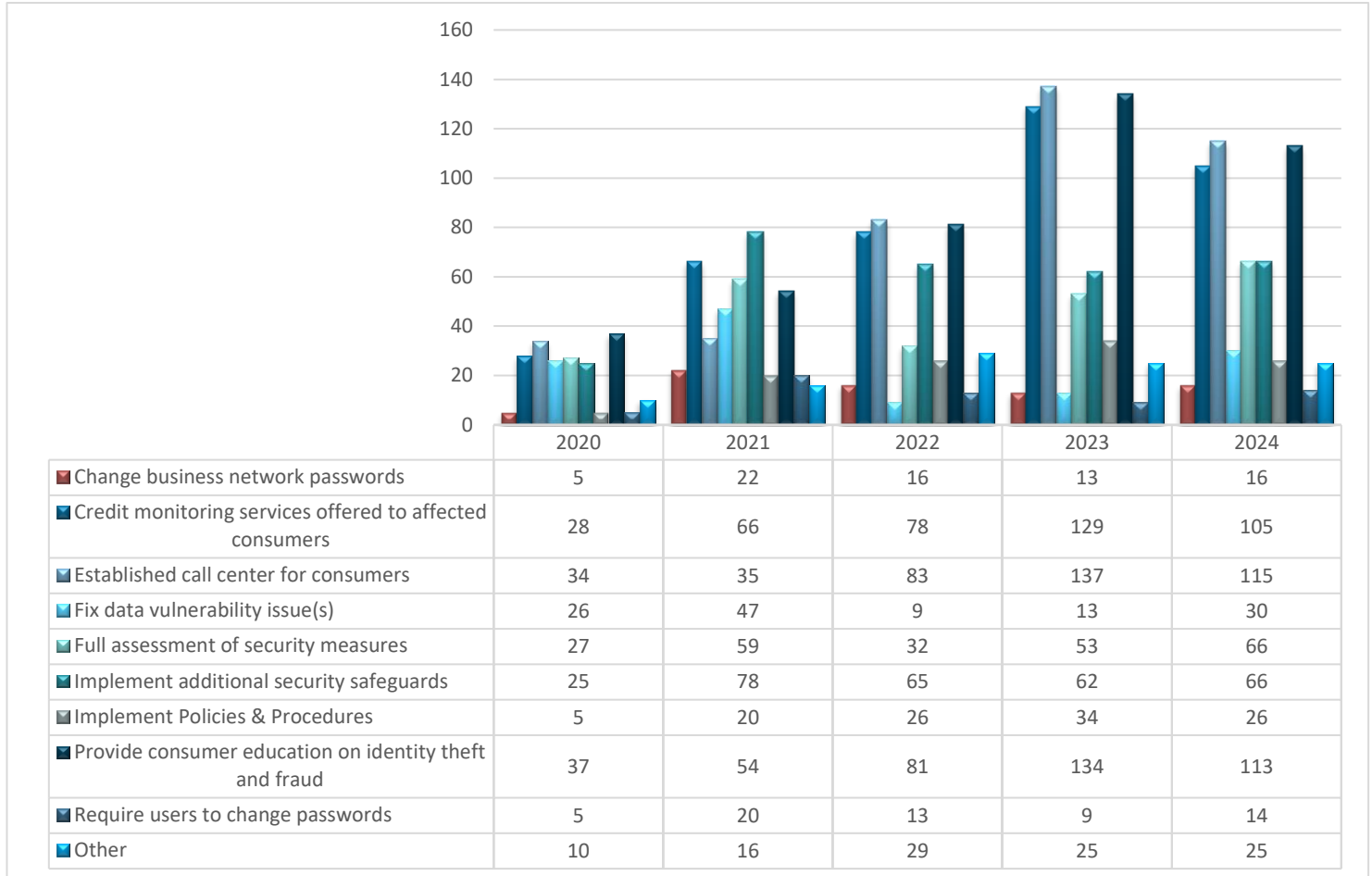
In 2024, SCDCA received fifty-two reports of security breaches due to unauthorized access, representing 43% of the total breaches reported for the year. Thirty-one security breach notices (26% of total) were due to hacking. Twenty-three security breach notices (19%) were due to a ransomware attack.

Types of Data Breached 2020 – 2024



From 2020 to 2024, SCDCA received 497 reports of security breaches. Of those, 483 (97.2%) reported breaches involved the exposure of protected personal data; 223 (46.9%) involved financial data; 163 (32.8%) indicated compromised protected health data; 81 (16.3%) implicated credential data; and 12 (2.4%) involved other types of potentially sensitive information. SCDCA’s methodology recognizes that multiple types of data can be breached within one security breach.

Remediation Steps Taken by Reporting Organizations 2020 – 2024



SCDCA’s methodology tracks multiple remediation steps taken by an organization in response to a security breach. For the 497 breaches reported 2020–2024, 81.7% offered free credit monitoring services to affected consumers; 84.3% provided consumer education on identity theft and fraud; 81.3% established a dedicated call center for affected consumers.

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.

