ISPARTNERS

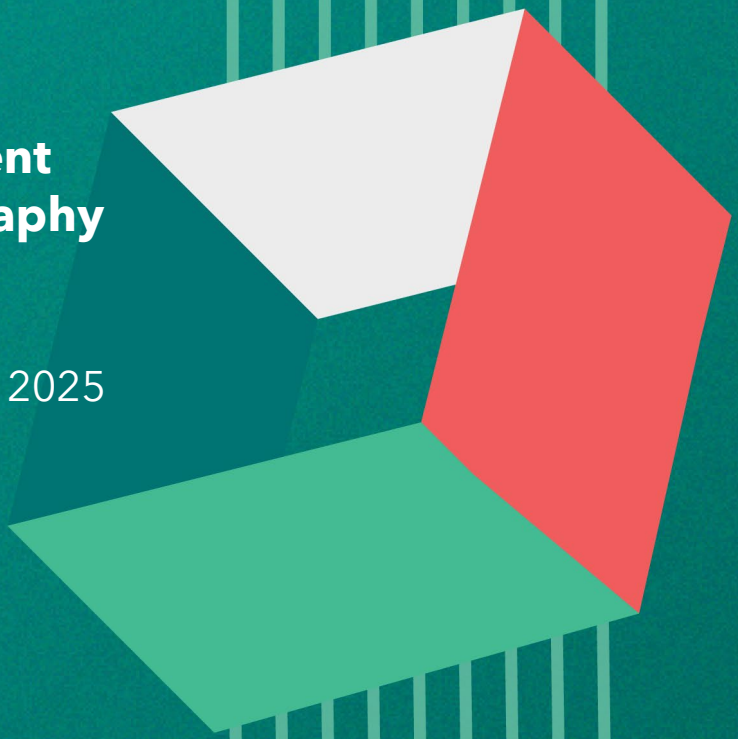
Lifetouch®

Report on Lifetouch's Management Assertion for the Digital Photography Products and Services System

January 1, 2025 through December 31, 2025

Relevant to Security

SOC 3®



I. INDEPENDENT SERVICE AUDITOR'S REPORT

ISPARTNERS

To the Management of Lifetouch:

Scope

We have examined Lifetouch's (the "Company") accompanying assertion titled "Management Assertion of Lifetouch" ("assertion") that the controls within Digital Photography Products and Services System ("system") were effective throughout the period January 1, 2025 through December 31, 2025, to provide reasonable assurance that Lifetouch's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus—2022)* (AICPA, *Trust Services Criteria*).

Service Organization's responsibilities

Lifetouch is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Lifetouch's service commitments and system requirements were achieved. Lifetouch has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Lifetouch is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed

IS Partners, LLC
1668 Susquehanna Road
Dresher, PA 19025

215.675.1400 main office
215.259.7928 fax
ispartnersllc.com

- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Digital Photography Products and Services system were effective throughout the period January 1, 2025 through December 31, 2025, to provide reasonable assurance that Lifetouch's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

IS Partners, LLC

IS Partners, LLC
Dresher, Pennsylvania
March 12, 2026

II. MANAGEMENT ASSERTION OF LIFETOUCH

Lifetouch

We are responsible for designing, implementing, operating, and maintaining effective controls within Lifetouch's Digital Photography Products and Services system ("system") throughout the period January 1, 2025 through December 31, 2025, to provide reasonable assurance that Lifetouch's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in this report and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025 through December 31, 2025, to provide reasonable assurance that Lifetouch's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus–2022)* (AICPA, *Trust Services Criteria*). Lifetouch's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in this report.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2025 through December 31, 2025, to provide reasonable assurance that Lifetouch's service commitments and system requirements were achieved based on the applicable trust services criteria.

Lifetouch,
March 12, 2026

III. DESCRIPTION OF THE BOUNDARIES OF LIFETOUCH'S DIGITAL PHOTOGRAPHY PRODUCTS AND SERVICES SYSTEM

Lifetouch

Company Background

For more than 80 years, Lifetouch has been the professional photography company of choice for schools and families. Headquartered in Eden Prairie, MN, the enterprise is organized around four primary business lines operating in local communities across North America.

Built on the tradition of "Picture Day," Lifetouch captures smiling faces from preschool through high school graduation, as well as sports, special events, seniors, and yearbooks. Additional photography services are offered through JCPenney Portraits by Lifetouch, helping families capture special milestones nationwide.

Lifetouch is also proud to be a part of the Shutterfly family of brands. For the purposes of this document, the term "Lifetouch" shall refer to Lifetouch and all shared corporate services as part of the Shutterfly family of brands, including Shutterfly subsidiaries, affiliates, and any entities that are controlled by, or under common control with Shutterfly, LLC.

Overview of the Services Provided

Lifetouch provides photography and yearbook services to schools through the underclass platform. The schools provide their roster data to Lifetouch and that is used to facilitate student photography in the schools. The images taken in the school, along with the student data, are used in the creation of products for the schools such as ID cards, creation of the yearbook and consumer products. The student roster data provided by the schools, as well as data provided by the consumer, includes personally identifiable information (PII). This data is covered by various state data privacy laws and by data privacy contracts with the schools. Lifetouch systems and processes work to maintain a level of security for the school and student data.

Locations

The following locations are in-scope for this audit:

- Eden Prairie, MN
- St. Paul, MN
- Lifetouch Labs
    - Winnipeg Lab: 1395 Inkster Blvd, Winnipeg MB R2X1P6
    - Galion Lab: 1371 OH-598, Galion, OH 44833
    - Muncie Lab: 601 W Ontario Drive Muncie, IN 47303

Principal Service Commitments and System Requirements

Lifetouch's objectives are based on the service commitments that Lifetouch makes to user entities, the laws and regulations that govern the provision of its solution, and the financial, operational, and compliance requirements that Lifetouch has established for the solution.

Regulatory Commitments
Due to the nature of the services Lifetouch provides and the data types it processes for schools; the organization's operations are impacted by requirements set forth in the Family Educational Rights and Privacy Act (FERPA). Policies, standards, and control programs are designed to ensure compliance with these regulatory requirements. An appropriate member of management reviews operating procedures for handling restricted data on at least an annual basis. The organization has formally documented procedures defining the procedure for handling protected student data.

Contractual Commitments
Vendor agreements are in place and agreed to between Lifetouch and external parties and vendors prior to the beginning of the relationship. Master service agreements (MSA) are used with all vendors. Specific subject matters such as confidentiality and ownership, information security, location security, and privacy considerations are included in the MSA. These agreements are signed prior to the commencement of the relationship.

Components of the System
The system is comprised of the following five components:

- Infrastructure
- Software
- People
- Procedures
- Data

The following sections of this description define each of these five components comprising Lifetouch's Digital Photography Products and Services system and other relevant aspects of Lifetouch's control environment, risk assessment process, information and communication systems, and monitoring controls.

Infrastructure
The Lifetouch environment is a hybrid cloud environment with systems hosted in local third-party data centers and systems hosted in AWS. The third-party data center environments use VMware to create virtual machines to run the applications. The third-party data center environments also host some applications on physical servers. The systems primarily use Oracle and MS SQL databases and Hitachi HNAS for storage. Messaging is accomplished through an Oracle Service Bus. The services are routed through an F5 load balancer.

AWS services are a combination of Elastic Beanstalk applications and Lambda functions. The primary database platform is a managed Aurora database (both MySQL

and Postgres are in use). The services make use of S3 for object storage and SQS for messaging. APIs made available externally reside behind the AWS API Gateway. We have the AWS Direct Connect service in place to facilitate communication between systems in the third-party data center and AWS.

All critical assets are identified and maintained in a central systems inventory. The organization uses a Confluence Wiki to track each asset and maintain a system inventory. The system inventory includes the following data points for each asset included in the inventory: asset description, asset location and asset owner. Each asset owner is responsible for ensuring that all information related to their assigned assets is current and accurate.

Software

Lifetouch has an inventory of critical software. The software inventory is managed within Atlassian Confluence. The organization has created an approved software list that provides details on the application and the most up-to-date software versions approved for use by the company.

People

Lifetouch is designed from a top-down approach in a traditional hierarchical structure with executive management at the head of the organization and is partitioned according to business function. Each of the primary functions is further broken down by department specialization. The Lifetouch division is headed by an SVP / Group Chief Executive. The information security and compliance teams are headed by a CISO who reports to the SVP / Chief Product and Technology Officer. A formal organization chart is maintained and visually represents Lifetouch's organizational structure. The organization chart is maintained in Employee Central (the organization's human resources platform) and is automatically updated within the system.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access

- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Data

Dataflows are documented to track how data enters, flows within the network, and is stored within the Lifetouch environment. The organization has a formally documented policy that addresses the classification of such data. The policy specifies that the data owner maintains the protection of the information asset according to the requirements specified by the data owner. The data owner is also responsible for ensuring that the information classification is assigned and properly indicates its business value, level of sensitivity, and criticality to the organization. Handling guidelines address information storage, transmission, and disposal. Information asset classifications are detailed within the policy as public, internal, confidential, or restricted data.

PII is defined as restricted data. The policy also documents roles and responsibilities, handling requirements, legal considerations, and information security requirements.

A retention schedule is used to identify how long each type of asset must be retained according to all applicable contractual, legal, and regulatory obligations. Information assets whose retention period is explicitly stated in the retention schedule or have a retention period specified by school contracts or the legal department must be destroyed within six months of the end date of the information asset retention period.

The organization has formally documented procedures that address the proper disposal methods for confidential material and the responsibility of each employee. The organization must maintain strict control over the storage and accessibility of media that contains restricted data; this includes maintaining detailed inventory logs and conducting media inventory reviews at least annually. Any media that contains restricted data and is no longer needed for business or legal reasons must be destroyed in a manner that renders the data unrecoverable. All media with a classification above public must be physically destroyed at the end of its usable life or no longer used or required.

Sensitive paper media is deposited in locked shred bins at the organization's office facilities, and all electronic media is placed in the server rooms at each of the facilities to be properly erased and disposed of.

The Data Management Policy, along with the Encryption Architecture Standard, outlines Lifetouch's methods for protecting data during storage and transmission. All data is encrypted using Transport Layer Security (TLS) when a session is established or when the company sends and receives data. Most data is encrypted at rest on all storage arrays used to store data and when data is backed up. Sensitive data must be encrypted when transmitted outside of the protected network environment. Public and internal data does not require encryption unless authorized by the Chief Information Security Officer. All passwords must be encrypted, and all non-console administrative access must be encrypted using technologies such as TLS, Secure Shell Protocol (SSH), or virtual private network (VPN) for web-based management.

The use of encryption must be limited to algorithms that have received public review and have been proven to work effectively and must comply with appropriate country, state, and local legislation and regulations; this includes all import and export laws. The use of digital certificates within the company must adhere to digital certificate standards.