CERTIFI User Manual

Compliant Electronic Receipt Transactions through Innovation and Financial Integrity

UNC | FINANCE AND OPERATIONS
Finance and Budget

Version: 3-27-2024

Contents

CERTIFI Overview

About CERTIFI

The Compliant Electronic Receipt Transactions through Innovation and Financial Integrity (CERTIFI) Committee is the clearinghouse for all compliance issues related to University credit card security. This cross-departmental Committee monitors Payment Card Industry Data Security Standard (PCI DSS) regulatory statutes and contractual obligations on behalf of university merchants.

The Committee is sponsored in partnership by Finance and Information Technology Services (ITS). CERTIFI is not responsible for student organizations or affiliates. Accounting Services, Information Security Office (ISO), and ITS Enterprise Applications provide support to CERTIFI and University merchants.

Website: Merchant Services

Email Address: certifi@unc.edu

What is Payment Card Industry Data Security Standard (PCI DSS)

Founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa, the Payment Card Industry Security Standards Council (PCI SSC) provides guidelines to protect cardholder data. The industry standard (Payment Card Industry Data Security Standards – PCI DSS) for maintaining security are communicated via six goals.

- Build and maintain a secure network.
- Protect cardholder data.
- Maintain a vulnerability management program.
- Implement strong access control measures.
- Regularly monitor and test networks.
- Maintain an information security policy.

The University created the Compliant Electronic Receipt Transactions through Innovation and Financial Integrity (CERTIFI) Committee to direct, manage, maintain, and ensure merchants' compliance with these goals.

What is a merchant?

A university department that accepts payment cards and electronic payments for services, fees, and/or goods.

What are a merchant's responsibilities?

- Maintain PCI compliance. Safeguard cardholder's payment card information.
- Ensure staff complete their annual PCI training. This training is administered online. It is the department's responsibility to ensure CERTIFI has an updated list of individuals required to take the PCI training.
- Ensure departmental staff are familiar with [Policy on Merchant Card Services](.).
- Enter the revenue into Connect Carolina daily by 10:00 am each business day.
- Complete a physical inventory of terminals as determined by the Internal Security Assessor (ISA).
- Complete the appropriate SAQ annually.

Self-Assessment Questionnaire (SAQ)

A Self-Assessment Questionnaire (SAQ) is a formal report of an organization's compliance with the Payment Card Industry Data Security Standard (PCI DSS). It evaluates whether a merchant or service provider has taken the necessary measures to secure cardholder data and documents its overall security posture.

Approved Merchant Types

Type	Characteristics
SAQ A	- Internet (online) Merchants. - Staff should **never** see or hear a credit card number. - All transactions are customer directed. **Never** instruct a customer to use a university device for payment purposes.
SAQ B	- Cellular point-of-sale terminal(s). - Payment card numbers should be entered directly into the terminal. - If payment cards are written down on paper they should be stored in a safe. After processing the payment, the card number should be cross-cut shredded. **Never** save payment card information in a spreadsheet or any electronic device.
SAQ Point-to-Point Encrypted (P2PE)	- Ethernet connected point-of-sale terminal(s) that encrypt payment card information at the swipe. - Payment card numbers should be directly entered into the terminal. - If payment cards are written down on paper they should be stored in a safe. After processing the payment, the card number should be cross-cut shredded. **Never** save payment card information in a spreadsheet or any electronic device.

Vendor Considerations

Does the vendor adhere to the daily deposit requirement?

The State of North Carolina has certain statutes in place that require vendor adherence. One of the statutes is related to the deposits of state funds.

G.S. 159-32 Page 1 § 159-32. Daily deposits.

(a) Except as otherwise provided by law, all taxes and other moneys collected or received by an officer or employee of a local government or public authority shall be deposited in accordance with this section. Each officer and employee of a local government or public authority whose duty it is to collect or receive any taxes or other moneys shall, on a daily basis, deposit or submit to a properly licensed and recognized cash collection service all collections and receipts. However, if the governing board gives its approval, deposits or submissions to a properly licensed and recognized cash collection service shall be required only when the moneys on hand amount to five hundred dollars ($500.00) or greater. Until deposited or officially submitted to a properly licensed and recognized cash collection service, all moneys must be maintained in a secure location. All deposits shall be made with the finance officer or in an official depository. Deposits in an official depository shall be immediately reported to the finance officer by means of a duplicate deposit ticket. The finance officer may at any time audit the accounts of any officer or employee collecting or receiving taxes or other moneys and may prescribe the form and detail of these accounts. The accounts of such an officer or employee shall be audited at least annually.(b) The Secretary may, during an emergency declaration issued under G.S. 166A-19.20,set the amount of moneys on hand requiring daily deposits and may require deposits on less than a daily basis, provided the moneys are maintained in a secure location and deposited at least weekly. (1927, c. 146, s. 19; 1929, c. 37; 1939, c. 134; 1955, cc. 698, 724; 1971, c. 780, s. 1;1973, c. 474, s. 27; 2017-204, s. 6.1(a); 2020-3, s. 4.28(a).)

§ 147-77. Daily deposit of funds to the credit of Treasurer.

All funds belonging to the State of North Carolina, in the hands of any head of any department of the State which collects revenue for the State in any form whatsoever, and every institution, agency, officer, employee, or representative of the State or any agency, department, division or commission thereof, except officers and the clerks of the Supreme Court and Court of Appeals, collecting or receiving any funds or money belonging to the State of North Carolina, shall daily deposit the same in some bank, or trust company, selected or designated by the State Treasurer, in the name of the State Treasurer, at noon, or as near thereto as may be, and shall report the same daily to the Treasurer. The State Treasurer may authorize exemptions from the provisions of this section so long as funds are deposited and reported pursuant to the provisions of this section at least once a week and, in addition, so long as funds are deposited and reported pursuant to the provisions of this section whenever as much as five thousand dollars ($5,000) has been collected and received. Each State agency that has custody of funds less than five thousand dollars ($5,000) shall provide adequate safekeeping of such funds. The Treasurer may refund the amount of any bad checks which have been returned to the department by the Treasurer when the same have not been collected after 30 days' trial. (1925, c. 128, s. 1; 1945, c. 159; 1969, c. 44, s. 77; 1985, c. 708; 2015-164, s. 3(b).)

Is UNC CH the merchant of record (MOR)?

A merchant of record (MOR) is the company that sells products or services to the final customer, and the legal entity those customers pay when making a purchase. The MOR takes on the fiscal responsibility and liability of payments, billing, sales, taxes, refunds, and chargebacks, and more.

Does the vendor use Fiserv as the processing bank?

The University of North Carolina at Chapel Hill relies upon The Office of State Controller's contract with Fiserv merchant bank for its payment card processing. Potential vendors are required to use Fiserv merchant bank for processing.

Is the vendor a TouchNet Ready Partner?

TouchNet is the University's preferred gateway. Merchants are required to use TouchNet. To learn more about TouchNet Ready Partners visit [TouchNet Partner Directory](#)

Does the vendor have a valid Attestation of Compliance (AOC) for their hardware and/or software?

A valid AOC has the following characteristics:

- The AOC is signed by a Qualified Security Assessor or Internal Security Assessor.
- The AOC is dated within the last 365 days.

Gateways are also required to have a valid AOC.

Preparing to Submit a Request to CERTIFI for Review

Checklist

Select the appropriate checklist from the appendix, based on the SAQ type, and confirm in partnership with the vendor that the request meets CERTIFI's requirements. Contact certifi@unc.edu for questions or to request a representative attend vendor meeting(s).

Submitting a Ticket to Data Governance (DGOG)

CERTIFI has partnered with DGOG to ensure requests for new merchants receive all the proper reviews.

DGOG routes requests to:

- CERTIFI for PCI reviews.
- Data stewards and Privacy Office to ensure federal and state privacy regulations are addressed appropriately. This includes information related to social security numbers, Health Insurance Portability and Accountability Act (HIPAA), Protected Health Information (PHI), and other types of data.
- Information Security Office for risk assessments.
- Registrar Office for The Family Educational Rights and Privacy Act (FERPA) reviews.
- Purchasing to ensure contracts are executed according to state law.

Glossary of Terms

Attestation of Compliance (AOC)

Software, hardware, gateway compliance documentation.

Gateway

Gateway is a network node used in telecommunications that connects two networks with different transmission protocols together. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.

Internal Security Assessor (ISA)

An official designation earned by an internal employee who has been trained to perform internal assessments and recommend solutions to remediate issues related to Payment Card Industry.

Merchant Application and Renewal (MAR) Document

The application CERTIFI uses to evaluate and review merchants.

Payment Card Industry (PCI)

The major card brands; American Express, Discover, Japan Credit Bureau, MasterCard, and Visa.

Qualified Security Assessor (QSA)

Companies are independent security organizations that have been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS. QSA Employees are individuals who are employed by a QSA Company and have satisfied and continue to satisfy all QSA Requirements.

SAQ A Checklist

Requirements

- ☐ Does the vendor meet the daily deposit requirement?

- ☐ Will UNC CH be the merchant or record (MOR)?

- ☐ Does the vendor use Fiserv as the processing bank?

- ☐ Is the vendor a ToucheNet Ready Partner?

- ☐ Does the vendor have a valid attestation of compliance?

- ☐ Submit a ticket to DGOG by visiting [Data Governance at UNC](#)

  - State that the request has PCI Components.

  - Request and Complete the MAR provided by CERTIFI.

- ☐ Complete The Office of State Controller paperwork.

SAQ B Checklist

Requirements

☐ Does the vendor meet the daily deposit requirement?

☐ Will UNC CH be the merchant or record (MOR)?

☐ Does the vendor use Fiserv as the processing bank?

☐ Does the device use cellular service? Wi-Fi service will not be approved.

☐ Does the vendor have a valid AOC?

☐ Submit a ticket to DGOG by visiting Data Governance at UNC

- State that the request has PCI Components.
- Request and Complete the MAR provided by CERTIFI.

☐ Complete The Office of State Controller paperwork.

SAQ P2PE Checklist

Requirements

- ☐ Does the vendor meet the daily deposit requirement?

- ☐ Will UNC CH be the merchant or record (MOR)?

- ☐ Does the vendor use Fiserv as the processing bank?

- ☐ Is the device PCI DSS validated Point-to-Point encrypted? Provide the PCI DSS listing.

- ☐ Does the vendor have a valid AOC for their hardware?

- ☐ Does the gateway have a valid AOC for their hardware?

- ☐ Submit a ticket to DGOG by visiting [Data Governance at UNC](#)

  - State that the request has PCI Components.

  - ☐   Request and Complete the MAR provided by CERTIFI.

- ☐ Complete The Office of State Controller paperwork.

DGOG Checklist

What do you need to include in the DGOG ticket?

☐ Note on the ticket that CERTIFI review is required.

☐ Provide a summary of the department's business need for the new hardware or software.

☐ Provide the amount of revenue the merchant will generate on an annual basis.

☐ Provide the proposed implementation date.

☐ Provide the names of individuals who need to attend the CERTIFI kickoff meeting. This should include individuals from the department's ITS team and accounting team.