United Community Banks, Inc.			
Document Title	Privacy Policy	**Version No.**	1
Effective Date	February 2023		
Date of Last Revision	January 2023		
Policy Owner	Chief Compliance Officer		
Reviewing Committee	Chief Compliance Officer and Risk Management Committee		
Approving Body	Board Risk Committee		

CONTENTS

1. Policy Statement and Scope

It is the policy of United Community Banks, Inc. ("UCBI" or "Company" or "we") to comply with all applicable laws, rules, and regulations with respect to all statutory provisions of the privacy rules and regulations in this Policy. Management and the Board will establish and maintain a corporate culture and business practices that ensure there are sufficient compliance controls in place including (but not limited to) policies and procedures, training, and monitoring and auditing functions to effectively identify program weaknesses that exist, ensure corrective measures are implemented, and provide Company management and the Board (or a committee thereof) with periodic reports of the program's status.

We maintain this Policy to help manage our potential compliance, legal, regulatory, and reputational risks associated with offering financial products and services to our customers.

This Policy applies to all activities and employees involved in the day-to-day activities related to information sharing between Company affiliates, non-affiliated third parties, and service providers and the requirements outlined in GLBA, Regulation P, and FCRA. Additionally, this Policy applies to personnel involved with information sharing activities under RFPA when UCBI receives an information request from the federal government about a UCBI customer. Finally, this Policy applies to personnel involved in the development, marketing, and/or servicing of products targeting children as outlined in COPPA, whether now or in any future product initiatives.

2. Governance, Roles, and Responsibilities

The following table describes the high-level roles and responsibilities applicable to the implementation, oversight, and review of this Policy.

Responsible Party	Role/Responsibility
UCBI Board Risk Committee ("Board Risk Committee")	The Board Risk Committee is responsible for: • Approving new and material revisions to this policy.
Risk Management Committee	The Risk Management Committee is responsible for: • Reviewing new and material revisions to this policy; and • Periodically receiving and reviewing reports to monitor compliance with this policy.
Chief Compliance Officer	The Chief Compliance Officer is responsible for: • Maintaining ownership of this Policy; • Overseeing and administering, or appointing an appropriate designee(s) to oversee and administer (in whole or in part) this Policy; and • Providing routine reporting and escalating Policy related issues or concerns to Business Unit Management, Board and Management Committees, and the Board, as appropriate.
Line of Business Senior Management	Line of Business Senior Management is responsible for: • Ensuring appropriate directives are implemented and administered in compliance with this Policy; • Working with Compliance and other Key Stakeholders to ensure that appropriate procedures are in place; and • Day-to-day oversight of the business processes and functions where the underlying regulatory requirements apply, and escalating any potential issues to Compliance or Legal.
All Employees	Employees involved in privacy related activities at UCBI are responsible for: • Having sufficient knowledge of the requirements of the laws, rules, and regulations in this Policy to ensure compliance with its provisions and to avoid violations which could subject UCBI to civil or criminal fines and penalties.
Audit	UCBI's Chief Audit Executive ("CAE") is charged with conducting periodic audits to ensure UCBI's compliance program effectively meets regulatory requirements. The CAE will present reports of such examinations to the Audit Committee of the Board of Directors.

3. PRIVACY PRINCIPLES

UCBI collects customer information from many different sources (e.g., opening deposit accounts, loans, or receiving other services), and this can include many types of information including (but not limited to) the customer's name, address, tax identification number, telephone number, date of birth, mother's maiden name, driver's license number, credit report information, employment status, income, assets, or liabilities, among other types of information.

As much of this information is Nonpublic Personal Information (NPI), UCBI has a regulatory and reputational responsibility to ensure this information is safeguarded and only shared within the allowable confines of the applicable privacy related laws and regulations. UCB recognizes the following eight elements of its privacy policy, which have become standard within the banking industry:

1. ***Recognition of Customer's Expectation of Privacy***: UCBI recognizes that our customers expect privacy and security of their personal and financial affairs. The need to safeguard sensitive information about our customers is critical; therefore standards and procedures of daily operations are designed to prevent misuse of this information.
2. ***Use, Collection, and Retention of Customer Information***: During the normal scope of business UCBI collects, retains, and uses information about our customers only when there is a reasonable belief that it will help administer their business or provide products, services, and other opportunities to them. It is our policy to collect and retain information about our customers only for specific business purposes – and it is a requirement to disclose the reason(s) for collecting and retaining it upon customer request. UCBI uses this information to protect and administer customer records, accounts, and funds; to comply with certain laws and regulations; to help design or improve products and services; and to understand our customers' financial needs so that we can provide them with quality products and superior service.
3. ***Maintenance of Accurate Information***: UCBI's daily operating procedures help assure that customer financial information is accurate, current, and complete in accordance with commercial standards and practices. It is our policy to respond to customer requests to correct inaccurate information in a timely manner. While some of these procedures are required by federal or state law, UCBI has adopted procedures to maintain accurate, current, and complete financial information, including processes to update information and remove old information.
4. ***Limiting Employee Access to Information***: All employees are required to follow the UCBI's Employee Handbook and applicable Information Security Policies in regards to accessing customer NPI. UCBI has implemented procedures that limit employee access to personally identifiable customer information to those employees with a business reason to know such information. UCBI will take appropriate disciplinary measures if an employee misuses NPI.
5. ***Protection of Information via Established Security Procedures***: UCBI is committed to the security of customer financial and personal information. UCBI's operational and data processing systems are maintained in a secure and redundant environment that protects customer account information from being accessed by third parties, and we maintain internal security standards and procedures to help prevent unauthorized access to confidential customer information. These security mechanisms are periodically updated and tested to improve the protection of customer information to assure the data integrity.
6. ***Restrictions on the Disclosure of Consumer Information***: It is UCBI's policy not to reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide corporate due diligence or business matter, unless:
    a. A customer requests or authorizes it;
    b. The information is provided to help complete a transaction initiated by a customer;
    c. The disclosure is required by or allowed by law (e.g., subpoena, investigation of fraudulent activity, request by regulator, etc.); or
    d. UCBI informs a customer about the possibility of disclosure for marketing or similar purposes through a prior communication and given the opportunity to decline (i.e., "opt-out").
7. ***Maintaining Customer Privacy in Business Relationships with Third Parties***: Sometimes it is necessary for UCBI to provide personally identifiable customer information to a contractual third party entity, such as a vendor or service company that is hired to prepare account statements or to provide support or services for one or more products. These vendors and service companies agree to safeguard confidential customer information regarding the products and services customers use by written agreement, and must abide by applicable law in doing so.
8. ***Disclosure of Privacy Principles to Customers***: UCBI will provide customers with a privacy notice at account opening, and thereafter as required by law. In addition, we make our Privacy Policy available on our website for customers to reference at any time.

4. Privacy Notices and Disclosures

a. Overview

The GLBA is a federal law enacted to control the ways that financial institutions deal with the private information of individuals. The Act regulates the collection and disclosure of private financial information and stipulates that financial institutions must implement security programs to protect such information. The Dodd-Frank Act granted authority to the Consumer Financial Protection bureau (CFPB) to examine and enforce compliance with the privacy rules with respect to entities under CFPB jurisdiction.

The purpose of Title V, Subtitle A of the GLBA and its implementing Regulation P is to inform consumers of the policies and practices of disclosing nonpublic personal information to affiliates and nonaffiliated third parties and to provide them with the option of opting out of certain sharing of information. The rules apply only to information about individuals who obtain financial products or services to be used for personal, family, or household purposes. The rules do not apply to information about businesses, corporations, partnerships, or similar entities or about individuals who obtain financial products or services for business purposes.

Additional provisions pertaining to GLBA's requirements to ensure the protection of customer information are detailed in the Bank's Information Security Policy.

The Fair Credit Reporting Act (FCRA) gives consumers the ability to stop the sharing of their credit application information or other personal information (obtained from third-parties, such as credit bureaus) with affiliated companies, and if we do share this type of information, it only allows UCBI to share such application or credit bureau information after we provide the customer a privacy notice and the opportunity to opt-out. FCRA also permits sharing of information with affiliates regarding the consumer's performance on the loan or other "experience" resulting from the relationship between the consumer and the financial institution.

b. Contents of Privacy Notice

The Privacy Notice will include (but is not limited to) the following information:

- How UCBI collects, shares and protects a consumer's information;
- Examples of types of information that may be collected, such as social security number, income, employment, account balances, and credit history;
- Reasons UCBI can share the information, such as for everyday business use,
- Marketing purposes and for affiliates business and marketing purposes;
- Whether or not UCBI does share the information; and
- Whether or not the customer can limit this sharing.

c. Initial Privacy Notice Requirements

At account opening, UCBI will provide a "clear and conspicuous" initial Privacy Notice to customers that accurately reflects our privacy policies and practices. The Privacy Notice will be designed to be reasonably understandable and to call attention to the nature and significance of the information contained in the notice.

The initial Privacy Notice will be provided in paper format unless the customer has agreed to receive the notice electronically under the E-Sign Act, and the most current version of the Privacy Notice will be retained on UCBI's website, and conform to the model disclosure established in the regulation.

d. Annual Privacy Notice Requirements

UCBI will provide an Annual Privacy Notice to existing customers as applicable in accordance with regulatory requirements, and only if the Bank's privacy policies and practices have changed since the last notice was provided. UCBI will also comply with this requirement if it makes a change to a policy or practice that triggers a revised notice.

The most current version of the Privacy Notice will be retained on the Bank's website, and conform to the model disclosure established in the regulation.

e. Privacy Opt-Outs

Currently, UCBI does not share information that would permit the consumer to opt out of information sharing. If this changes in the future, this Policy will be updated and procedures will be implemented to ensure compliance with the opt-out requirements.

5. Right To Financial Privacy Act (RFPA) Policy Requirements

a. Overview

The RFPA establishes procedures that federal government agencies must follow in order to obtain confidential customer information. The procedures are designed to balance the federal government's need for information when conducting a criminal investigation with the customer's right to privacy. The RFPA describes when the federal government may obtain financial records, the financial institution's obligations, and the customer's rights. The RFPA requires financial institutions to ensure the requirements are met prior to releasing customer information to a government agency.

Regulation S (Subpart A) establishes the rates and conditions for reimbursement of reasonably necessary costs directly incurred by financial institutions in assembling or providing customer financial records to a government authority.

b. General Requirements

No government agency may access or obtain any customer information maintained by UCBI unless the customer information that is being requested is reasonably described and at least one of the following is provided to UCBI:

- An administrative or judicial subpoena or summons;
- A search warrant;
- A formal written request; or
- A customer's written authorization.

i. Administrative or Judicial Subpoena or Summons

Upon receipt of a request for financial records made by a Government authority pursuant to an administrative subpoena or summons or pursuant to a judicial subpoena, UCBI shall, unless otherwise provided by law, proceed to assemble the records requested and will deliver the records to the Government authority upon receipt of the required written certification that it has complied with the applicable requirements of the RFPA.

A Government authority may obtain financial records pursuant to an administrative subpoena or summons otherwise authorized by law only if:

- Such subpoena is authorized by law and there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry;
- A copy of the subpoena or summons has been served upon the customer or mailed to his last known address on or before the date on which the subpoena or summons was served on the financial institution together with a notice which shall state with reasonable specificity the nature of the law enforcement inquiry; and
- Ten days have expired from the date of service of the notice or fourteen days from the date of mailing of the notice to the customer and within such time period the customer has not filed a sworn statement and motion to quash in an appropriate court, or the customer challenge provisions have been complied with.

ii. Search Warrants

A government agency may obtain customer information if it obtains a search warrant pursuant to the Federal Rules of Criminal Procedure.

iii. Formal Written Requests

UCBI will honor a Formal Written Request if:

- The request is authorized by regulations and signed by the head of the agency or department;
- No administrative summons or subpoena reasonably appears to be available to that government agency to obtain customer information for the purpose in which they are sought;
- There is reason to believe that the records are sought relevant to a legitimate law enforcement inquiry;
- The customer has been served a copy of the request or one has been mailed to the last known address on or before the date the request was made to the bank, together with a notice stating with reasonable specificity, the nature of the law enforcement inquiry; and

- Ten days have expired from the date of service or 14 days from the date of mailing and within such period the customer has not filed a sworn statement and application to enjoin the government agency in the appropriate court.

iv. Customer's Written Authorization

UCBI will honor a customer's written authorization if UCBI receives a signed and dated statement which:

- Authorizes such disclosure for a period not in excess of three months;
- States that the customer may revoke such authorization at any time before the information is disclosed;
- Identifies the specified information that is authorized to be disclosed;
- Specifies the purposes for which, and the government agency to which, such information may be disclosed; and
- States the customer's rights under the RFPA.

v. Delayed Notice to Customer

The customer notice may be delayed by order of an appropriate court if:

- The investigation being conducted is within the lawful jurisdiction of the government agency seeking the information;
- There is reason to believe that the information being sought is relevant to a legitimate law enforcement inquiry; and
- There is reason to believe that such notice will result in:
  - Endangering the life or physical safety of any person;
  - Flight from prosecution;
  - Destruction of or tampering with evidence;
  - Intimidation of a potential witness; or
  - Otherwise seriously jeopardizing an investigation or official proceeding or unduly delaying a trial or ongoing official proceeding.

c. Regulation S Cost Reimbursement

When reimbursements for costs associated with providing financial records to a government agency are requested, UCBI will take the appropriate measures to ensure that the government agency reimburses only for reasonably necessary costs directly incurred in searching for, reproducing or transporting books, papers, records, or other data. The Bank will follow the reimbursement schedule found in Appendix A to Regulation S and reimbursement costs allowed under the State of Georgia.

6. The Children's Online Privacy Protection Act Policy (COPPA) Policy Requirements

a. Overview

COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. The primary goal of COPPA is to place parents in control over what information is collected from and about their children online. For purposes of this policy, "children" are individuals under the age of 13.

UCBI recognizes that protecting children's identities and privacy online is important and the responsibility to do so rests with both the online industry and the parents. In the event that UCBI desires in the future to market or solicit such information, UCBI shall develop and implement appropriate policies and procedures prior to such initiatives.

b. Collection of Personal Information

UCBI will not knowingly gather personal information from a child through online means, including but not limited to:

- Requesting children submit personal information online (i.e. first and last name, home or other physical address, including street, email address or other online contact information; telephone number; or social security number). This includes minimum age restrictions on UCBI's online account opening platform;

- Enabling children to make personal information publicly available through a chat room, message board, or other means, except where UCBI deletes all individual information from postings by children before they are made public and also deletes such information from the Bank's records.

7. Policy Administration

The Policy Owner is responsible for final Policy content and is available for consultation on Policy interpretation. This Policy and its supporting procedures should be interpreted in a manner consistent with all applicable laws, rules, and regulations. Any apparent conflicts between this Policy and laws, rules, and regulations must be escalated immediately to the Policy Owner for further evaluation.

8. Approval Requirements

The Policy Owner shall review this Policy annually, or more frequently if revisions are required. At a minimum, the Policy Owner shall submit the Policy for review and approval to the Board Risk Committee. This Policy is effective following final approval. The Policy Owner is authorized to make minor or non-substantive alterations to this Policy, such as job titles or grammatical changes, without requiring Board Risk Committee review and approval.

9. Enforcement and Implementation

All Personnel are responsible for complying with this Policy. Non-compliance may be subject to disciplinary action. Exceptions to this Policy are generally not permitted unless authorized by the Policy Owner. The Policy Owner must only grant exceptions on a limited, case-by-case basis and only when compensating Controls are in place. The Policy Owner must provide routine Policy exception reporting to Business Unit Management, committees, and the Board, as appropriate.

10. Ongoing Monitoring and Oversight

The Policy Owner must be able to demonstrate adherence with this Policy using established monitoring and oversight routines. Management is responsible for ensuring that non-compliance with Policy requirements are appropriately escalated to ensure appropriate visibility of risks relating to this Policy. The Policy Owner must also provide routine reporting to escalate risks, issues, or concerns to Business Unit Management, committees, and the Board, as appropriate. Reporting may include, but is not limited to, revisions to this Policy and/or documented issues, concerns, or non-compliance with this Policy.

11. Review and Revision History

Review Date	Reviewed By	Review or Revision Description	Approved or Adopted	Approved or Adopted Date
January 2023	Board Risk Committee	Updated to New Policy Template; Combined Regulation P Privacy Policy, RFPA Policy, and COPPA Policy	Approved	02/14/2023

APPENDIX I: GLOSSARY

For purposes of this Policy, these terms are defined as follows:

Business Units	Any organizational units within the Bank that: (i) engage in activities designed to generate revenue; (ii) provide information technology, operations, servicing, processing, collections, or other specialized support to such organizational units, or (iii) provide general support services, such as administration, finance, treasury, or human resources for any such organizational unit. By engaging in these activities, these Business Units create risks to the Bank. For the avoidance of doubt, the Legal Department is not considered Business Unit.
Compliance Department	UCB's Compliance Department
Consumer	An individual who obtains or has obtained a financial product or service from a bank that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. An example of a consumer would be a loan applicant. A consumer is not necessarily a customer.
Control	A policy, procedure, process, or other manual or automated mechanism designed to prevent, detect, deter, identify, mitigate, or correct Compliance Risk.
Customer	A person who has established a "continuing relationship" with the bank. (For example, an approved loan applicant who signs a note would become a customer).
Nonpublic Personal Information	Nonpublic personal information is "personally identifiable financial information that is provided by a consumer to a financial institution, results from any transaction with, or service performed, for the consumer or is otherwise obtained by the financial institution. The rule excludes 'publicly available information' from the definition of nonpublic personal information. Publicly available information is any information that an institution has a reasonable basis to believe is lawfully made available to the general public from government records, widely distributed media, or disclosures to the public required to be made by federal, state, or local law. To have a reasonable basis, the institution must determine three things: ▪ Whether the information is of the type available to the general public, ▪ Whether an individual may direct that the information not be made available to the general public, and ▪ If the individual may so direct, whether he or she has not made the information available." An interpretation of this would be any information that is not available to the general public and/or associates a consumer with a particular institution. For example, a customer's name and address are public information, however a customer's name and address associated with a particular financial institution is not (which means the fact that a customer has a relationship with the bank cannot be released to someone else). Financial institutions must protect the information they receive from consumers when that consumer performs any transaction or utilizes any service offered by the financial institution.

Personnel	Employees, contractors and temporary staff, and Third Party Service Providers performing any activity for, or on behalf of, UCBI.
Policy Owner	The employee that owns this Policy and operationalizing, monitoring, and enforcing Policy on Policies expectations.
Publicly Available Information	Any information that a bank has a reasonable basis to believe is lawfully made available to the general public from Federal, State, or local government records; widely distributed media; or disclosures to the general public that are required to be made by Federal, State, or local law. (For example, a published telephone directory, or the public record of real estate transactions.)
UCBI or Company	United Community Bank, Inc.

APPENDIX II: KEY LEGAL REQUIREMENTS

Key laws, rules, or regulations that apply to this Policy include, but are not limited to, the following:

- 15 U.S.C. Sections 6801-6809
- 12 CFR Part 1016 - Privacy of Consumer Financial Information (Regulation P)
- FIL 01-106: Privacy of Consumer Financial Information
- Fixing America's Surface Transportation Act of 2015, Pub. L. No. 114-94 (2015), 129 Stat. 1312 (2015)
- FDIC Examination Manual – Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)
- CFPB – Privacy of Consumer Financial Information - Gramm-Leach-Bliley Act (GLBA) examination procedures
- Right to Financial Privacy Act of 1978: 12 USC §§3401 – 3422
- Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505