TCFA Presentation

July 14, 2022

OCCC

TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

OCCC
TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Compliance and Agency Updates

OCCC

TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Texas Consumer Installment Loan Data Trends

Preliminary 2021 data

(as of 6/30/2022)

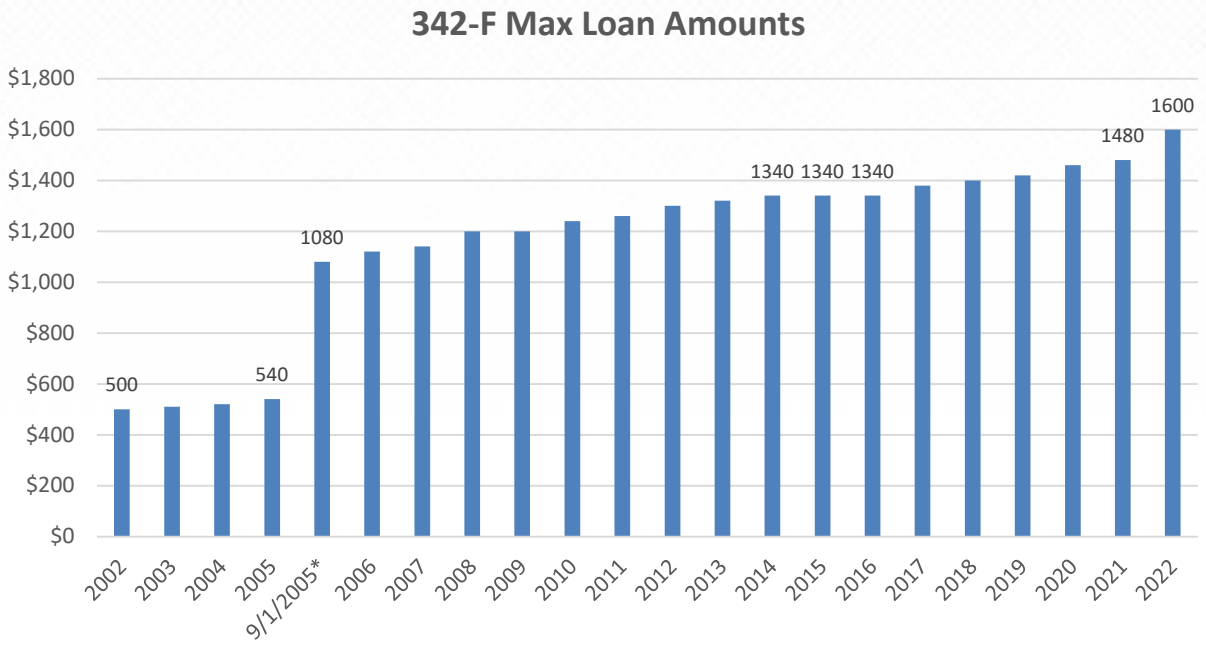
Loan Bracket Updates – effective July 1, 2022

342-F Max Loan Amounts

- Increased from $1,480 to $1,600 *(8.11% yearly increase)*
- $500 to $1,600 *(220% increase since 2002)*

Acts 2005, 79th Leg., Ch. 1018 (H.B. 955)

Doubled the maximum cash advance effective 9/1/2005



OCCC
TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Economic Forecasts & Trends

Leading Indicators

Consumer Confidence Index decreased 23.4% *(Texas Consumer Confidence decreased 26.3% for the same period)*

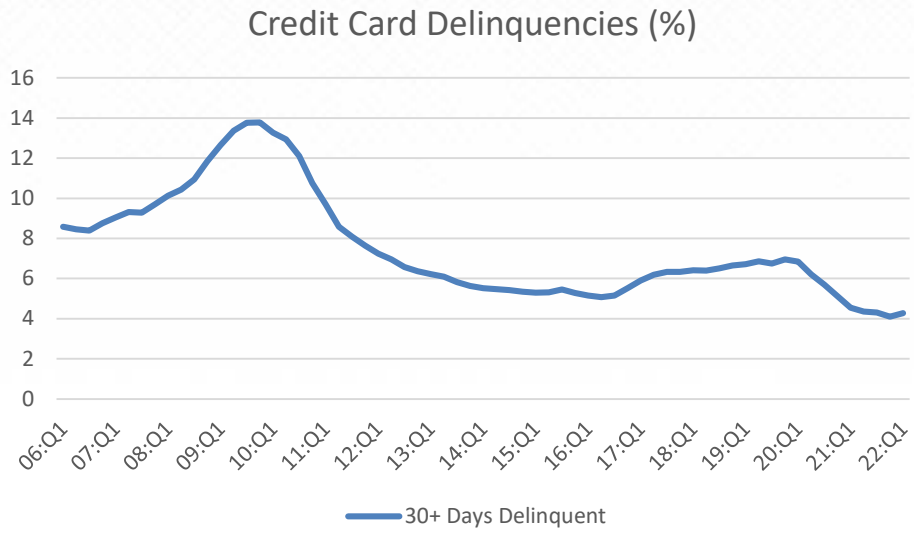
Texas Residential Single Family Building Permits decreased 6.4% 12 months ending in May while Multi-family permits increased 64.3%

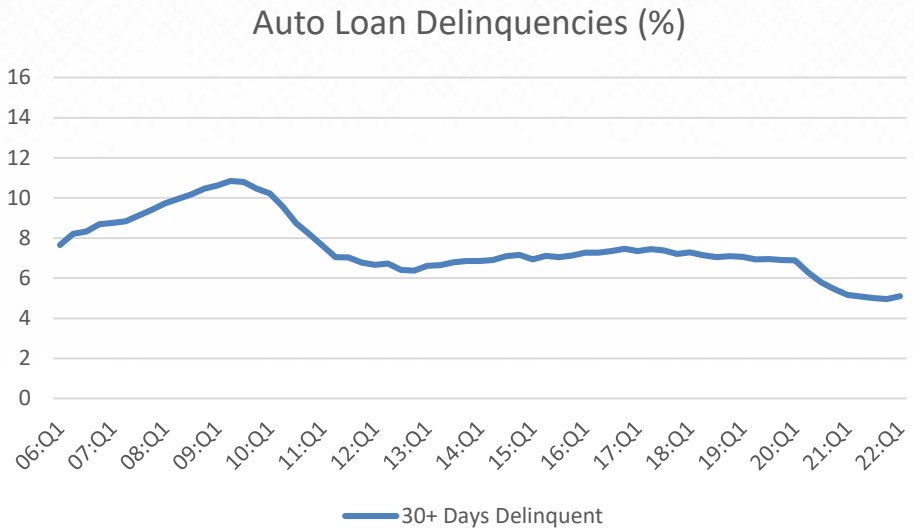
Lagging Indicators

CPI was up 1.0% in May and 8.6% over 12 months *(Texas CPI was up 9.0% for 12 months)*

The unemployment rate remains unchanged at 3.6% in May *(Texas increased 10 basis points)*

National Credit Delinquencies

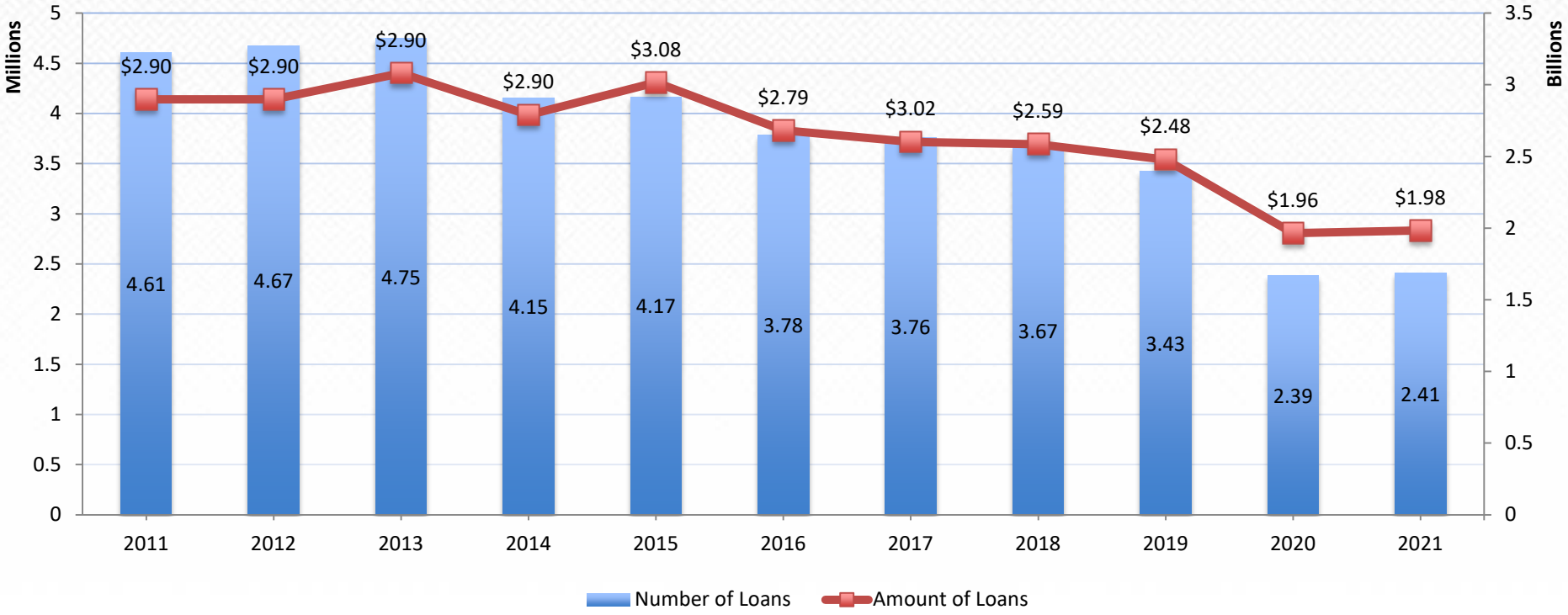




OCCC
TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Historical Report Data - Small Installment Loans (342-F)

342-F Loans Made

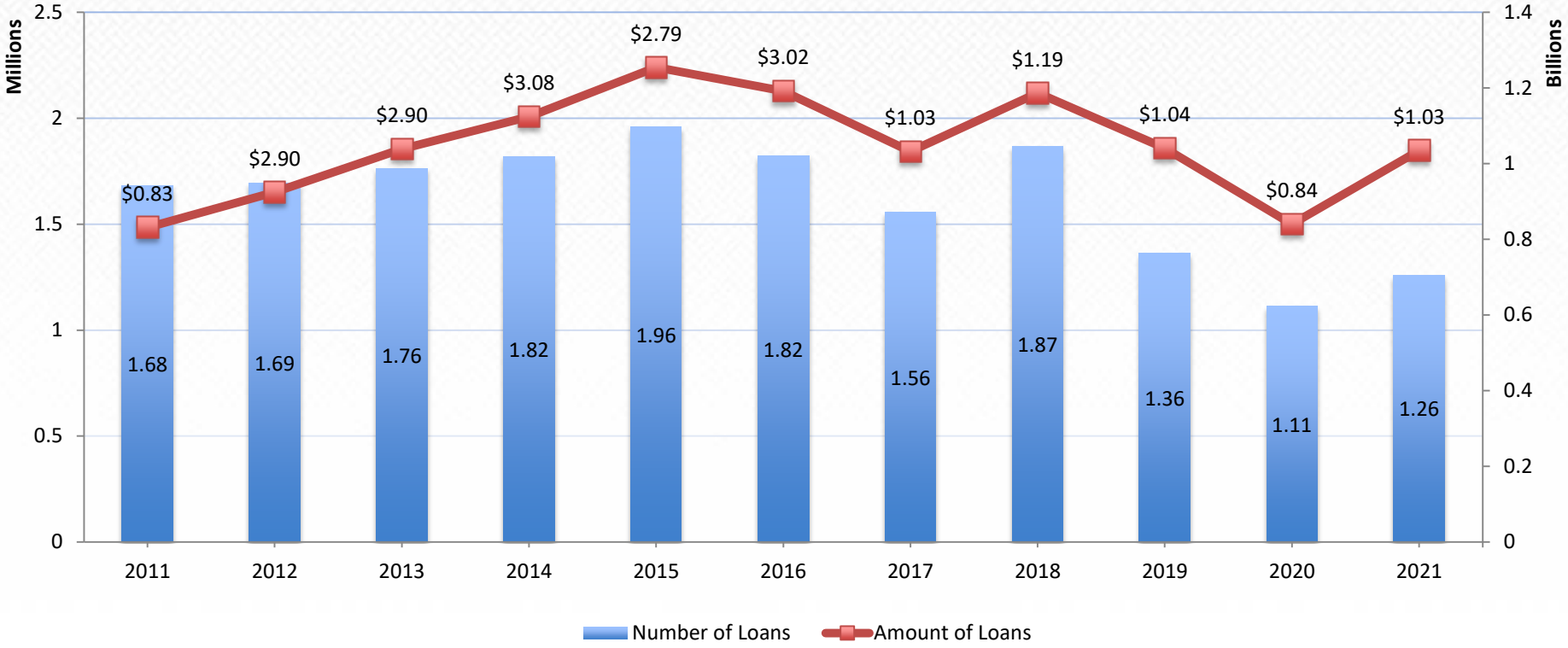


*Preliminary data through 6/30/2022

OCCC
TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Historical Report Data - Small Installment Loans (342-F)

Loans Receivable

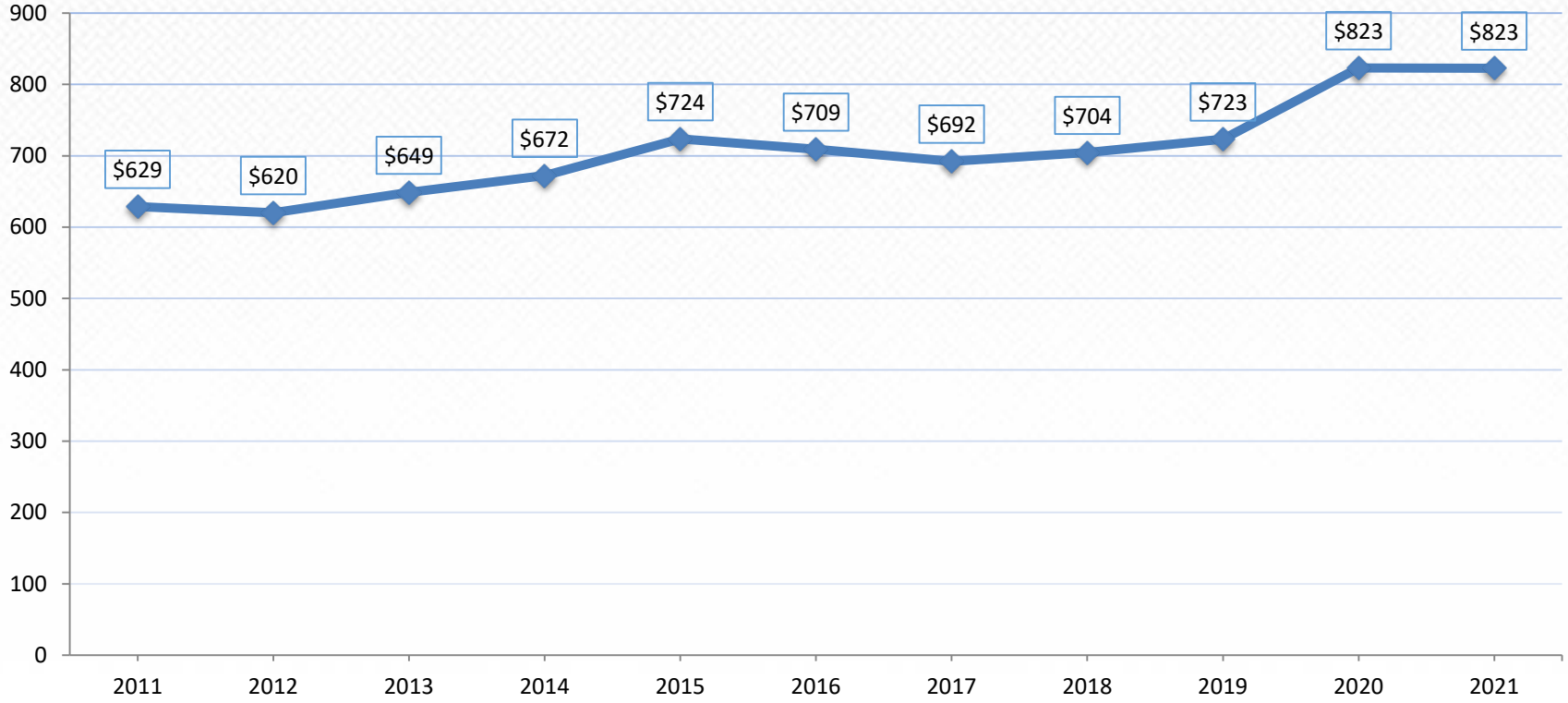


Preliminary data through 6/30/2022

TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Historical Report Data - Small Installment Loans (342-F)

Average Loan Amounts

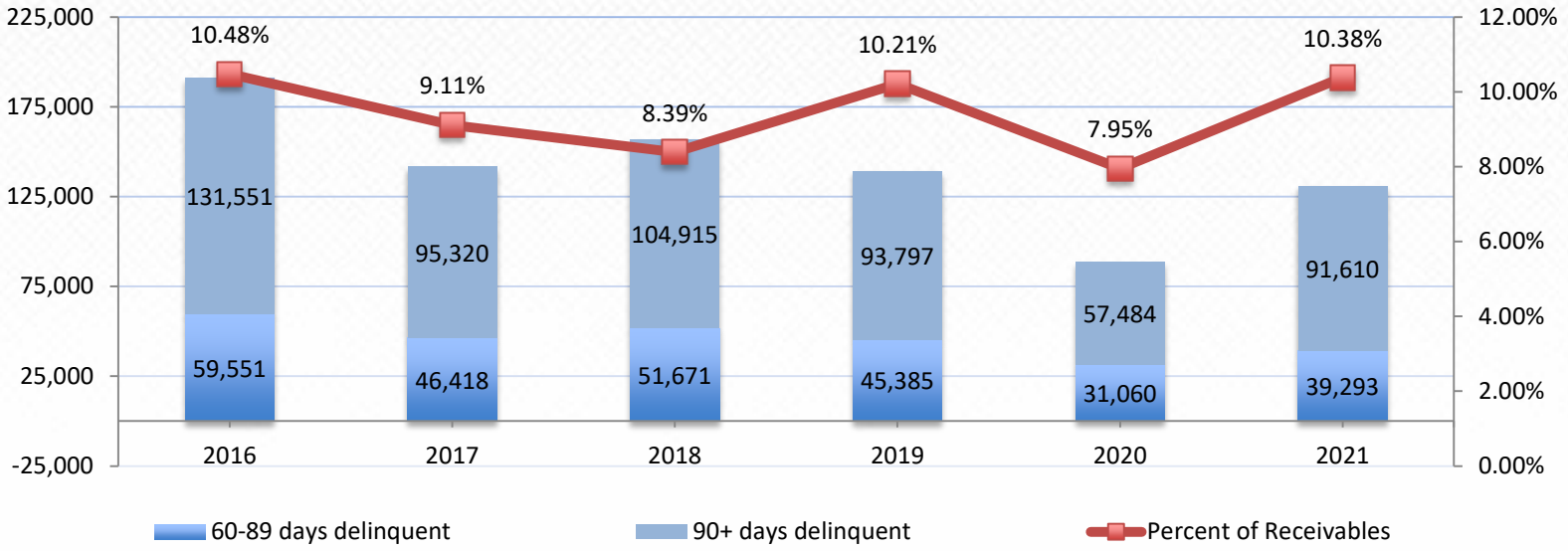


*Preliminary data through 6/30/2022

OCCC
TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Historical Report Data - Small Installment Loans (342-F)

Number of Delinquent Regulated Loans*

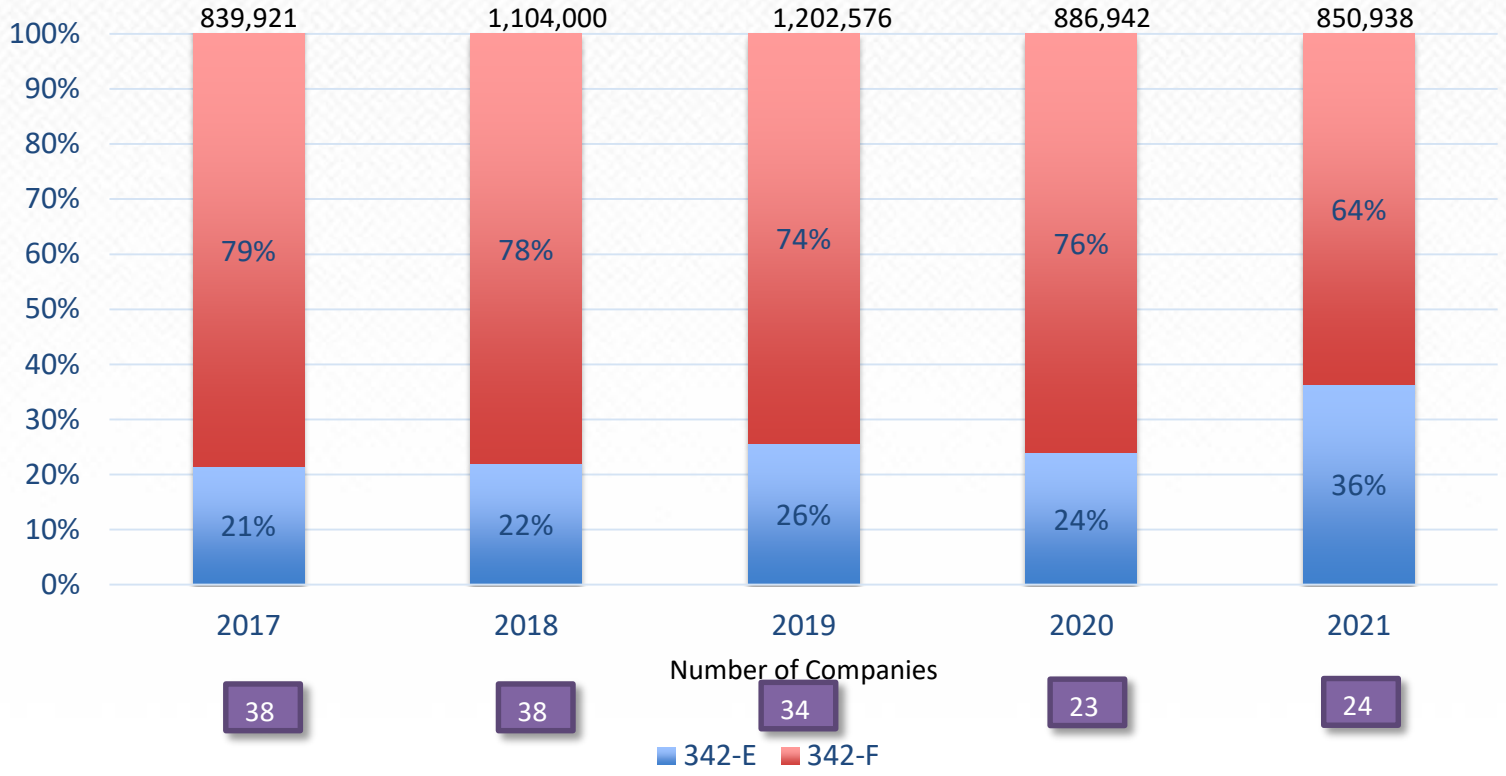


*May include other types of Regulated Loans
data as of 6/30/2022

Companies with Multiple Product Lines

Companies Making both 342-E and 342-F Loans

(Total loans, Percentage by Type, and Number of Companies)

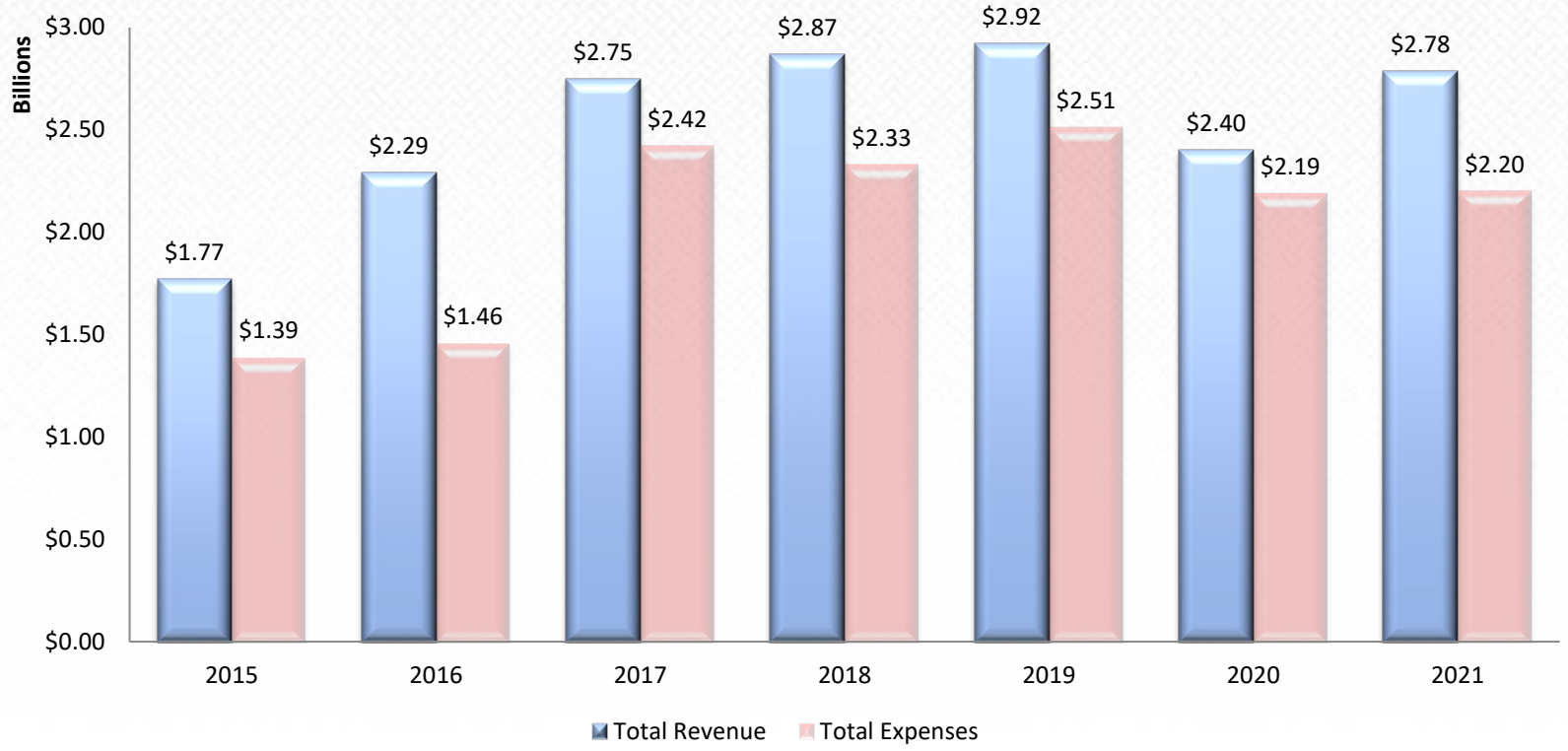


Data as of 6/30/2022

OCCC
TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Historical Income Statement (342-F Companies)

Total Income (company wide)



Data as of 6-30-2022. Includes income and expenses from all business activity.

FTC Safeguards Rule

What Your Business Needs to Know

https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know#Financial_institution

OCCC

TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Safeguards Rule – Brief History

Congress enacted the Gramm Leach Bliley Act ("GLB" or "GLBA") in 1999. The GLBA provides a framework for regulating the privacy and data security practices of financial institutions. Among other things, the GLBA requires financial institutions to

1. Provide customers with information about the institutions' privacy practices and about their opt-out rights *(privacy notice)*
2. To implement security safeguards for customer information

Safeguards Rule – Brief History

The Federal Trade Commission promulgated the Safeguards Rule (16 CFR part 314) in 2002 (effective date one year later in 2003) that sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Safeguards Rule – Brief History

The original Safeguards Rule required financial institutions to:

- "develop, implement, and maintain a comprehensive information security program . . . appropriate to size and complexity, the nature and scope of activities, and the sensitivity of any customer information at issue."
- This comprehensive program must be coordinated by one or more individuals and based on a risk assessment.

Safeguards Rule – Brief History (need for updating)

Why was the Rule revised?

1. Two decades of technological advances have changed how institutions collect and store information
2. The original rule lacked specificity in certain areas for setting standards to follow

Safeguards Rule – Updated

The Modified Safeguards rule was published on 12/09/2021 (with most new provisions taking effect on 12/09/2022) which modifies the previous rule in five primary ways.

1. *Sets forth more detailed requirements for the information security program.*
2. *Improves accountability of information security programs, by requiring the designation of a Single Qualified Individual and requiring periodic reports to the board of directors.*
3. *Exempts small financial institutions (those that collect information on fewer than 5,000 customers) from requirements of written risk assessment, incident response plan, and annual reporting to board of directors.*
4. *Broadens the definition of Financial Institution (specifically "finders" that bring together customers and the providers of a product or service) to include additional entities.*
5. *Includes definitions and related examples in the rule without having to reference the related privacy rule*

Specific Provisions Effective December 9, 2022

Many of the changes to the rule have delayed implementation that is effective December 9, 2022.

314.4(a) -- Single Qualified Individual

314.4 (b)(1) -- Written Risk Assessment

314.4(c)(1) through (8) – Access Control, Encryption, Multi-Factor Authentication, Audit Trails, Change Management, Disposal Procedures

314.4(d)(2) – Continuous Monitoring or Penetration Testing and Vulnerability Assessment

(e) – Training and Use of Qualified Information Security Personnel

(f)(3) – Periodically Monitor and Assess Service Providers

(h) -- Written Incident Response Plan, and

(i) -- Written Report to Board of Directors by Qualified Individual

Section 314.4(a) and (i) – Qualified Individual (Effective December 9, 2022)

Designate Qualified Individual

Designate a qualified individual ("QI") responsible for overseeing and implementing your information security program. The "QI" may be employed by you, an affiliate, or a service provider.

The QI must report in writing regularly – and at least annually – to your Board of Directors or governing body. If your company doesn't have a Board or its equivalent, the report must go to a senior officer responsible for your information security program.

Conduct a Risk Assessment

Your information security program must be based on a ***written*** risk assessment and must include criteria for:

1. Evaluation and categorization of identified security risks or threats you face

2. Assessing the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face.

3. Describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

Section 314.4(c)(1) (8)– Control the Risks Identified in Your Security Assessment (Effective December 9, 2022)

Design and Implement Safeguards

1. Implement and periodically review access controls (which employees have access to and is there a legitimate business need for it)
2. Know what you have and where you have it (periodic inventory of data and keep an accurate list of all systems, devices, and personnel)
3. Encrypt customer information on your system and when it's in transit (if not feasible, secure by an alternative method approved by the QI)
4. Assess your apps (procedures for evaluating security for apps you use)
5. Implement multi-factor authentication for anyone accessing customer information on your system

Section 314.4(c)(1) (8)– Continued (Effective December 9, 2022)

6. Dispose of customer information securely. (If you no longer have a business need you should dispose of customer records following the statutory recordkeeping schedule – *4 years from the date of loan or 2 years from the date of final entry)*

7. Anticipate and evaluate changes to your information system or network (Build a change management system to evaluate how new systems can affect the overall security of other established systems).

8. Maintain a log of authorized users' activity and keep an eye out for unauthorized access. (Have procedures and controls to monitor when authorized users are accessing customer information and to detect for unauthorized access)

Section 314.4(d)(2) – Monitoring and Testing (Effective December 9, 2022)

Monitor and Test Your Safeguards

Test your procedures for detecting actual and attempted attacks through either:

1. Continuous monitoring or;
2. Annual penetration testing and vulnerability assessments every 6 months

Train Your Staff

Implement policies and procedures to ensure that personnel are able to enact your information security program

1. Provide Security Awareness Training
2. Update Training as Necessary to Reflect Changes in Risk Assessment

Section 314.4(f)(3) – Monitor Service Providers (Effective December 9, 2022)

Monitor Your Service Providers

Periodically assess your service providers based on the risk they present and the continued adequacy of their safeguards. Contracts with service providers should specify:

1. Your security expectations
2. Ways to monitor their work
3. Reassessment of their suitability

Develop an Incident Response Plan

Establish a **written** Incident Response Plan that addresses :

1. The goals of your plan;
2. The internal processes your company will activate in response to a security event;
3. Clear roles, responsibilities, and levels of decision-making authority;
4. Communications and information sharing both inside and outside your company;
5. A process to fix any identified weaknesses in your systems and controls;
6. Procedures for documenting and reporting security events and your company's response; and
7. A post-mortem of what happened and a revision of your incident response plan and information security program based on what you learned.

Safeguards Rule Takeaways

Prior to 12/09/2022:

1. Compare existing information security programs to the revised Rule, and address any gaps.
2. Designate a Qualified Individual to be accountable for the program.
3. Make sure program materials and plans are in writing and are followed.

Added specificity in the rule brings an opportunity for uniform compliance, making sure all companies are following the same guidelines, and safeguarding information.

OCCC

TEXAS OFFICE OF CONSUMER
CREDIT COMMISSIONER