2015 Hot Topics

Iris Ikeda, Commissioner
Division of Financial Institutions
DCCA
June 2015

Topics

- TILA-RESPA Integrated Disclosure Rule (TRID)
- Privacy
- Cybersecurity
- Exam hot topics

TILA-RESPA Integrated Disclosure Rule

- Created by CFPB as mandated by the Dodd-Frank Act
- New forms:
  - The Loan Estimate form
  - The Closing Disclosure form
- Created to use clear language and design
- Applies to most closed-end consumer mortgages by creditors
- Not to HELOCs, reverse mortgages, mobile homes, land
- Effective date: August 1, 2015

What is the TRID about?

- Consolidates 4 existing disclosures under TILA & RESPA for closed-end credit transactions secured by real property
- Loan Estimate form must be delivered or placed in the mail no later than the 3rd business day after receiving the consumer's application
- Closing Disclosure must be provided to consumer at least 3 business days prior to consummation

What's covered by TRID?

- Covers most closed-end consumer credit transactions secured by real property
- Applies to trusts for tax or estate planning
- Not to HELOCs, reverse mortgages, mobile homes or land transactions

Record retention requirements

- Creditors:
  - Closing Disclosure and all documents related to the closing disclosure for 5 years after consummation
  - Post Consummation Escrow Cancellation Notice (Escrow Closing Notice) for 2 years
  - Loan Estimate and all documents for 3 years after consummation
- Records can be maintained by any method for 7 years (HRS)

Effective date & Transition

- New TRID effective August 1, 2015 for applications received by a creditor or MLO
- Creditors can use GFE, HUD-1 and TILA forms for applications received prior to Aug 1
- Use TRID forms as applications received after Aug 1 are consummated, withdrawn, or cancelled
- Creditors cannot use the TRID before Aug 1

What happens on Aug 1

- Restrictions on activity before the consumer's receipt of the Loan Estimate form
  - Imposing fees on a consumer
  - Customer must indicate an intent to proceed with the transaction
  - Providing written estimates on terms
  - Requiring the submission of documents verifying info related to the consumer's application

What transactions are not covered?

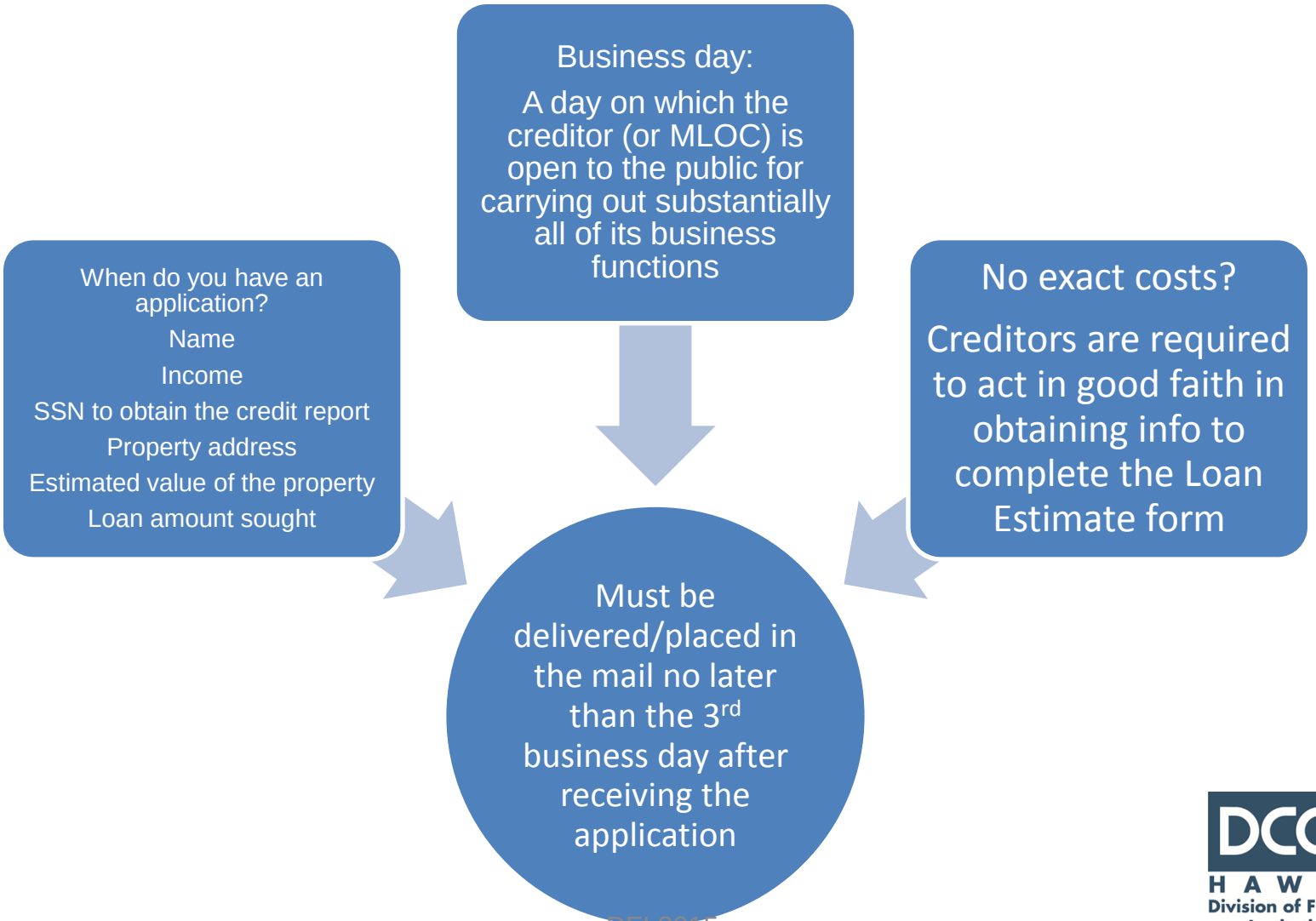
TRID applies

- Most closed-end consumer credit transactions secured by real property
- Construction only loans
- Vacant land of 25 or more acres
- Partial – housing assistance loan programs for low & mod income consumers

TRID does not apply

- HELOC
- Reverse mortgages
- Mobile homes
- Persons who are not creditors (a person or entity that makes 5 or fewer mortgages
- Use TILA/RESPA forms

Loan Estimate form



- QUESTIONS?

Privacy

Information is transmitted when it moves from one person or place to another. Examples of information transmission include but are not limited to:

- Written Correspondence
- E-Mail
- Voice Mail
- Information posted or submitted on or through the Internet or on internal Intranet
- FAX transmissions
- Telephone conversation
- Business meetings
- Presentations
- Wires and ACH transactions
- Scratch Paper, “sticky notes”

Identity Theft

- Identity theft is one of the fastest growing white-collar crimes in the U.S. Banks absorb most of the economic losses from credit and deposit account fraud associated with theft of consumer identities. The combination of these facts makes identity theft a significant issue for MLOCs and a risk that every MLOC employee must be constantly aware of and continuously seeking to deter and detect.

- Identity theft is the fraudulent use of an individual's personal identifying information. Often, identity thieves will use another individual's personal information such as name, social security number, driver's license number, mother's maiden name, date of birth or account number, to fraudulently open new credit card accounts, charge existing credit card accounts, write checks, open bank accounts or obtain new loans.

ID theft

Identity thieves use various techniques to steal the information. The following are examples of the most common techniques:

- Impersonating victims in order to obtain information from banks and other businesses;
- Stealing wallets that contain personal identification information and credit cards;
- Stealing bank statements from the mail;
- Diverting mail from its intended recipients by submitting a change of address form;
- Rummaging through trash for personal data;
- Stealing personal identification information from workplace records; or,
- Intercepting or otherwise obtaining information transmitted electronically.

Social Engineering

Social engineering is the attempt to manipulate or trick a person into providing confidential information to an individual that is not authorized to receive such information.

Four common types of social engineering techniques:

1) pretext calling;
2) dumpster diving;
3) shoulder surfing; and
4) identity theft.

Cyber Security

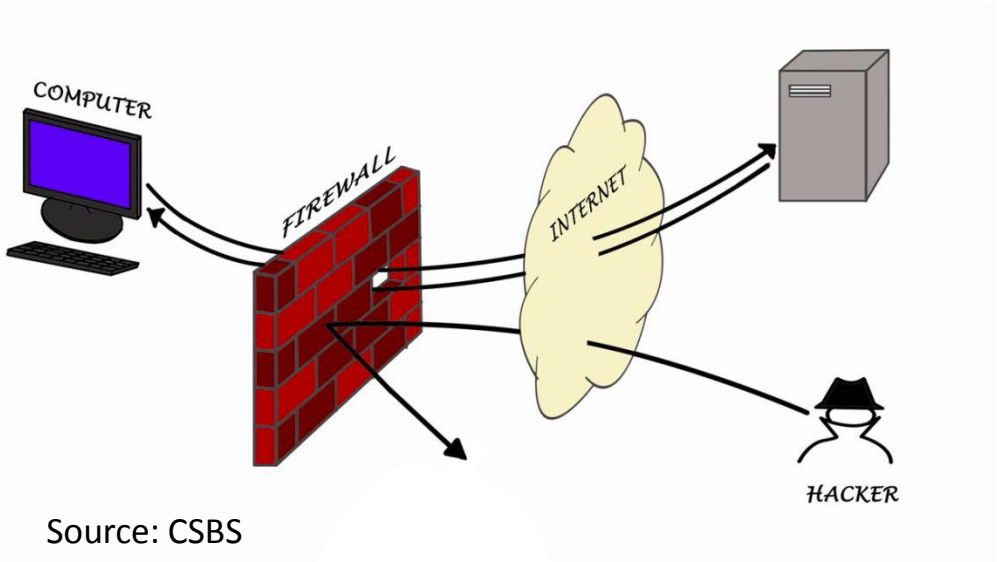
- IDENTIFY internal and external cyber risks
- PROTECT organizational systems, assets, and data
- DETECT system intrusions, data breaches, and unauthorized access
- RESPOND to a potential cybersecurity event
- RECOVER from a cybersecurity event by restoring normal operations & services

Cyber: IDENTIFY

- Risk assessment
  - Classify your “crown jewels”
  - Identify threats & vulnerabilities
  - Measure risk
  - Communicate risk

Cyber: PROTECT

- **Cyber hygiene:**
  - Steps computer users take to protect and maintain systems & devices.
- Customer authentication
- Access controls
- Data security



Source: CSBS

Cyber: DETECT

DETECT tools are the reinforcement of the Protect tools

- Intrusion Detection Systems;
- Network Behavior Anomaly Detection Tools;
- Security Information and Event Management /Log Analyzer;
- Configuration Management Tools; and
- Integrity Monitoring Tools.

Cyber: DETECT examples

Common cyber-attacks that bank CEOs should particularly know about and understand are:

- Distributed Denial of Service (DDoS) attacks;
- Corporate Account Take Over (CATO) attacks; and
- CryptoLocker attacks.

Cyber: RESPOND

Cybersecurity data breaches are now part of our way of life.

- **The Incident Response Plan**
- **Communicating the Data Breach**
  - **State law on notification**
- **You've Been Hacked/Attacked, What Are Your Next Steps?**
- The following are three steps to consider:
  - Triage/Evaluate the Cyber-event;
  - Invoke the Incident Response Plan; and
  - Review the effectiveness of the plan.

Cyber: RECOVER

- Restore & Review

- QUESTIONS?

Exam Hot Topics

- Virtual offices
- BSA
  - 4 pillars (internal controls, independent testing, BSA officer, training)
- Office hours
  - By appointment only
  - Signage

Exam Hot Topics – Virtual Offices

- Hawaii Safe Act requires a physical office

Exam Hot Topics - BSA

- Internal Controls – to ensure compliance
  - Policy – not complicated
    - Customize to your business
    - Include OFAC
  - Procedures – write down how you monitor
  - Risk Assessment – simple is best
    - Customized to your business
    - Who are your clients

Exam Hot Topics - BSA

Independent Testing

- Must be completed by a qualified party;
- Must be independent (in-house or external);
- Should be conducted every 12 to 18/24 months, depending on risk profile; and
- Can be a risk-based process.
- Report
  - Period of review
  - Name of Reviewer
  - Area of Review
  - Findings
  - Recommendations

Exam Hot Topics - BSA

BSA Officer

- Must be qualified;
- Must have sufficient authority, knowledge, and resources; and
- Is responsible for ensuring overall BSA compliance.

Exam Hot Topics - BSA

Training

A training program must be documented and should:

- Be tailored to specific job duties;
- Address regulatory requirements;
- Reference company policies, procedures, and processes;
- Be performed on an ongoing basis; and
- Reiterate employee responsibilities.

Exam Hot Topics - BSA

CIP (Customer Identification Program)

- Must form a reasonable belief of customer identity;
- Must include account opening procedures and verification methods;
- Must ensure collection of minimum data elements; and
- May use risk-based procedures for additional documentation and verification of customer identity.

Exam Hot Topics – Office Hours

Each location shall be open for business to the public during posted business hours.

Commercial buildings: the business hours shall be posted on or adjacent to the main office door of the MLOC location, and visible to the public from outside the location.

Non-Commercial building or posting not permitted: the business hours shall be posted on the home page of the MLOC's website, along with the address and phone number of the location.

Business hours, whether posted at a location or on a mortgage loan originator company website, shall be displayed in a clear, conspicuous, and accurate manner to inform the consumer when the location will be open.

- Questions?

What's next?

Act 64 (2015) - Permits the Commissioner of Financial Institutions to make adjustments to the collection of fees for the Mortgage Loan Recovery Fund without regard to Chapter 91, HRS

Rulemaking process continuing.

What's next?

Hawaii DFI is the 18th state in the nation to receive the CSBS/AARMR Mortgage Accreditation.

Confirms that DFI maintains the highest standards and practices in mortgage supervision set by the CSBS/AARMR Mortgage Accreditation Program.

What's next?

Contact us:

- www.cca.hawaii.gov/DFI
- Dfi-nmls@dcca.hawaii.gov
- Twitter - @HawaiiDFI

Tools –

Presentation will be on DFI website shortly