2.1 Notification concerning Principals (12/12/24)

In addition to the requirements set forth below, Chapter 7 sets forth Freddie Mac's requirements regarding fraud detection, prevention and reporting.

If a Seller/Servicer obtains knowledge of commission by a Principal of any act or offense indicating a lack of business competence, integrity or honesty, the Seller/Servicer must immediately

- Cease involving the Principal in any of the Seller/Servicer's Freddie Mac business, and
- Notify the Multifamily Fraud Investigative Unit in writing at MF_Mortgage_Fraud_Reporting@freddiemac.com.

Such knowledge includes knowledge of a criminal conviction or civil judgment against any Principal for commission of fraud or a criminal offense in connection with negotiating, obtaining, attempting to obtain, or performing a public or private agreement or transaction; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, perjury, making false statements, misrepresentation, receiving stolen property, conspiracy, making false claims, or obstruction of justice.

2.2 Limitation on the number and amount of Mortgage purchases and commitments (10/07/02)

Freddie Mac reserves the right to limit the number and/or aggregate dollar amount of Mortgage commitments it will accept from any Seller. Maximums are subject to change by Freddie Mac at any time without notice or publication.

2.3 Limitation on the number and amount of multifamily Mortgages (12/15/20)

Freddie Mac reserves the right to limit the number and/or aggregate dollar amount of multifamily Mortgages it will purchase within any geographic area, or with the same Borrower, Borrower Principal, or with related persons or Affiliates of the Borrower or Borrower Principal (including partnerships or corporations with common, interlocking, or interconnected ownership or organizational structures).

2.4 Sale of Mortgages by Freddie Mac (12/05/03)

Freddie Mac may from time to time sell, in whole or in part, Mortgages it has purchased pursuant to the Purchase and Servicing Documents. Freddie Mac will attempt to make the sales in a manner that causes as little disruption as possible to the Servicer.

2.5 Modification of programs and products (12/05/03)

Freddie Mac reserves the right to supplement, modify or terminate any purchase program or product at any time without prior notice.

2.6 Race or racial composition of a neighborhood (12/05/03)

Freddie Mac does not consider race and the racial composition of a neighborhood to be reliable appraisal factors. Freddie Mac will not purchase any Mortgage supported by an Appraisal report that makes reference to race or the racial composition of the neighborhood.

2.7 Freddie Mac audit (12/12/24)

Freddie Mac may, at any time, conduct an audit of a Seller/Servicer that is selling or Servicing Mortgages for Freddie Mac for the purpose of verifying the Seller/Servicer's compliance with the terms and conditions of the Purchase and Servicing Documents. Freddie Mac will select the Mortgages to be audited.

a. Before the audit (09/14/23)

Freddie Mac will inform Seller/Servicers who are scheduled to be audited that they must provide certain documentation to the Freddie Mac Multifamily Audit Lead through the Document Management System (DMS) or such other system or method as Freddie Mac may approve. The Servicer must provide the requested documentation within the applicable time frame(s) stated in the engagement letter that Freddie Mac sends to the Seller/Servicer before Freddie Mac's audit begins.

b. After the audit (12/12/24)

After the audit, Freddie Mac will prepare a written draft audit report that summarizes the audit and includes audit findings, if any, and provide such draft audit report to the Seller/Servicer.

Upon receipt of the draft audit report, the Seller/Servicer must immediately prepare a written response. The Seller/Servicer must send the response to the Freddie Mac Multifamily Audit Lead through email, DMS or such other system as Freddie Mac may approve within five Business Days after the Seller/Servicer's receipt of the draft audit report. The response must include a detailed remediation plan to resolve each finding identified in the audit. Freddie Mac will review the Seller/Servicer's written response and include it in the final audit report.

If the Seller/Servicer fails to provide a timely response, or the response does not adequately address each finding identified in the audit, or the Seller/Servicer fails to resolve an audit finding satisfactorily within 180 days of final audit report issuance and provide evidence of satisfactory remediation to the audit team within that time frame, Freddie Mac may:

- Increase its audit frequency, and/or
- Exercise any of its rights (as described in Chapter 4) to impose Probation or Suspension or Termination

Minor findings must be remediated, with evidence of remediation provided to Freddie Mac, within 180 days of issuance of the final audit report. The time frame for remediation of major and critical findings will be dictated by Freddie Mac and communicated to the Seller/Servicer.

See also the provisions in Chapters 46SBL and 47.

2.8 Receipt and treatment of confidential information (12/07/04)

Freddie Mac may provide the Seller/Servicer with information and documentation that Freddie Mac has identified as "confidential information" or "confidential." Such confidential information includes information and documentation concerning the development, negotiation, operation or terms of various products, programs, technology, business terms, trade secrets, certain commercial and financial information, and "material inside information" within the meaning of the federal securities laws. Confidential information may also include confidential information belonging to third parties.

1. The Seller/Servicer must treat all confidential information and all information or materials prepared from confidential information, defined as "derivative information," as strictly confidential and proprietary. The Seller/Servicer must not release or disclose or permit the release or disclosure of all or any part of the confidential information or the derivative information for any purpose at any time except to the extent:

   - Allowed by this section
   - Expressly required or consented to by Freddie Mac in writing, or
   - Ordered by a court or administrative agency

   In the event the Seller/Servicer anticipates that it may be required, for any reason, to release or disclose confidential information or derivative information, the Seller/Servicer must immediately notify the applicable *Freddie Mac Multifamily Attorney* to allow Freddie Mac to take any actions it deems necessary to prevent or limit the release or disclosure of the confidential information or derivative information.

2. Unless the Seller/Servicer has obtained prior written consent from Freddie Mac, the Seller/Servicer must not copy or permit copies to be made of all or any part of the confidential information or the derivative information except to the extent necessary for Servicing the Mortgages or fulfilling any other obligations to Freddie Mac. The Seller/Servicer must mark "Confidential" in a prominent location on all confidential information, derivative information and on all copies.

3. The Seller/Servicer may provide confidential information or derivative information to those officers, directors, principals, partners or employees of the Seller/Servicer and its regulators, auditors, counsel and accountants to the extent necessary to Service the Mortgages. The Seller/Servicer must notify any individuals receiving confidential information or derivative information that the individual has the same obligations as the Seller/Servicer to keep the confidential information or derivative information confidential.

4. Confidential information and derivative information do not include any information that is:

   - Generally available to the public
   - Provided to the Seller/Servicer by a third party that is not itself under a confidentiality obligation with respect to the information, or

- Independently developed by the Seller/Servicer without use of any portion of the confidential information

2.9 Availability of Freddie Mac Multifamily Loan Documents and other legal forms (02/29/12)

a. Freddie Mac Multifamily Loan Documents (02/29/12)

Freddie Mac Multifamily Loan Documents are available to Seller/Servicers in the Multifamily Loan Documents section of mf.freddiemac.com/lenders/legal/.

b. All other legal forms (02/29/12)

Freddie Mac legal forms that are not available at mf.freddiemac.com/lenders/legal/ are available from the applicable Freddie Mac *Multifamily Attorney*.

2.10 Co-marketing with the Freddie Mac Multifamily and Optigo® name, logo and offerings (06/27/19)

a. Optigo® Lenders (06/27/19)

1. Approval to use the Freddie Mac Multifamily and Optigo® logos

   A Seller/Servicer approved as an Optigo Lender may use the Freddie Mac Multifamily and Optigo logos or graphics in advertising, marketing or other promotional materials, provided that the Optigo Lender has provided Freddie Mac with a copy of the materials and Freddie Mac has approved those materials prior to their use.

2. Approval to use the Freddie Mac Multifamily and Optigo names

   Without review by Freddie Mac Multifamily, a Seller/Servicer approved as an Optigo Lender may use the name “Freddie Mac Multifamily” or “Optigo” in advertising, marketing or other promotional materials to indicate that it is approved to sell loans to Freddie Mac Multifamily, as long as those materials do not indicate that it is approved to sell a particular type of loan for which it does not have approval. Loan types include Conventional, Targeted Affordable Housing, Seniors Housing, and SBL Mortgages.

   If the materials are being used for any purpose other than to indicate approval to sell Freddie Mac Multifamily loans, then prior to using these materials, the Optigo Lender must provide Freddie Mac with a copy of the materials for Freddie Mac’s review and approval.

3. Approval to use Optigo offering terms and other offering information

   An Optigo Lender may use Optigo offering terms and offering information in whole or in part in its branded marketing materials if the following conditions are met:

   - The Optigo Lender has not modified any Freddie Mac Multifamily or Optigo trademarks or registered marks.

- The Optigo Lender has not changed any program terms.
- The Optigo Lender has provided Freddie Mac with a copy of the materials prior to their use.
- Freddie Mac has approved the provided materials.

4. Approval to link to online Freddie Mac resources

   An Optigo Lender may post direct web links from its branded webpage to Optigo program terms located on mf.freddiemac.com.

5. Freddie Mac's obligation to notify Optigo Lenders regarding changes

   If an Optigo Lender uses Freddie Mac offering terms or information in its marketing materials or posts direct web links from its webpage, it is the obligation of the Optigo Lender to keep the program terms and web links updated. Freddie Mac may modify, update or discontinue its product terms and other information or change its product terms located on its website from time to time. Freddie Mac is under no obligation to notify Optigo Lenders of any such changes beyond Freddie Mac's standard communications to all Freddie Mac Seller/Servicers regarding such changes.

b. Seller/Servicers not approved to sell to Freddie Mac (06/27/19)

A Seller/Servicer that is not an Optigo Lender may not use the Freddie Mac Optigo or Multifamily name, logo or offering information in any advertising, marketing or other promotional materials without the prior written consent of Freddie Mac.

c. Other entities (06/27/19)

An Optigo Lender that enters into a relationship with other entities for the purpose of originating multifamily Mortgages for sale to Freddie Mac must obtain, on behalf of those entities, the prior written consent of Freddie Mac before the other entities may use the Freddie Mac Multifamily or Optigo names, graphics or logos in advertising, marketing or other promotional materials. Such entities may not use these items without Freddie Mac's prior written consent.

d. Delivery of materials or requests for approval (06/27/19)

Optigo Lenders must submit requests to use the Freddie Mac Multifamily or Optigo graphics to the Freddie Mac Corporate Branding Group via the "Logo Use Permission" section of mf.freddiemac.com, http://www.freddiemac.com/terms/logo_use.html.

Optigo Lenders must send co-marketing requests, including requests to use the Freddie Mac name, to Multifamily Marketing at the multifamily_marketing@freddiemac.com.

Requests for consent must include a copy of the proposed material.

e. Withdrawal of approval (06/27/19)

Freddie Mac may withdraw an approval to use the Freddie Mac Optigo Lender designation, the Freddie Multifamily or Optigo logo, the Freddie Mac Multifamily or Optigo name, graphic, web link or product terms at any time upon 10 Business Days' prior notice. After receipt of such notice, the Optigo Lender must discontinue use of the designation, logo, name, graphic, product terms and/or web links, as applicable. However, if the withdrawal of the consent is required by Freddie Mac's regulators or any other governmental entity, Freddie Mac may withdraw the consent with such prior notice as is commercially reasonable or practicable under the circumstances. Upon receipt of notice that Freddie Mac is withdrawing its consent at the requirement of a regulator or other government entity, the Optigo Lender must promptly and diligently use good faith efforts to discontinue use of the product terms and/or web links, as applicable.

2.11 Minority-owned and women-owned business enterprises (06/27/19)

It is Freddie Mac's policy to provide the maximum practicable opportunity to minority-owned and women-owned business enterprises to compete fairly as suppliers, contractors and subcontractors in Freddie Mac's business activities, taking into account both price and quality. As an aspect of this policy, Freddie Mac encourages Optigo Lenders to ensure that minority-owned and women-owned business enterprises are given the opportunity to compete fairly in supplying services to our Optigo Lender network.

2.12 Using the Freddie Mac Multifamily Software Applications (02/18/21)

a. Authorization to use the Freddie Mac Multifamily Software Applications and Freddie Mac Approved Third Party Applications (02/18/21)

Freddie Mac authorizes each Seller/Servicer to use the Freddie Mac Multifamily Software Applications, at no cost to the Seller/Servicer, in connection with the sale of Mortgages to and/or the servicing of Mortgages for Freddie Mac, solely for the delivery of information and documentation to Freddie Mac. The Freddie Mac Multifamily Software Applications include the following:

- Consent Request Tracker (CRT)
- Document Management System (DMS)
- Freddie Mac Access Manager (FAM)
- General Loan Information (GLI)
- Insurance Compliance Tool (ICT)
- Multifamily Eligibility System (MES)
- Multifamily Securities Investor Access tool (MSIA)
- Multifamily Seller/Servicer Guide via AllRegs® Online (Guide)
- myOptigo℠
- Origination and Underwriting System (OUS)
- Property Reporting System (PRS)
- Small Balance Loan Production Pipeline Manager (PPM)

Freddie Mac further authorizes each Seller/Servicer to use Freddie Mac Approved Third Party Applications for the delivery of information and documentation to Freddie Mac. Such Freddie Mac Approved Third Party Applications may require the Seller/Servicer to enter into

a contract for services with the applicable third party. Seller/Servicer remains solely responsible and liable for, and Freddie Mac undertakes no responsibility and/or liability in connection with, any error, omission, malfunction and/or negligence caused by Seller/Servicer's use of Freddie Mac Approved Third Party Applications.

Freddie Mac Approved Third Party Applications include the Optigo Happy Inspection Application, powered by HappyCo.

Freddie Mac agrees to accept information and documentation through the Freddie Mac Multifamily Software Applications and Freddie Mac Approved Third Party Applications.

b. Seller/Servicer's use of the Freddie Mac Multifamily Software Applications and Freddie Mac Approved Third Party Applications (09/30/20)

The Seller/Servicer's use of the Freddie Mac Multifamily Software Applications and Freddie Mac Approved Third Party Applications must comply at all times with the requirements of the Guide and any user manuals and instructions provided by Freddie Mac.

c. Seller/Servicer's warranties (09/30/20)

The Seller/Servicer acknowledges that all of the representations and warranties that it is deemed to make under Chapter 5 of the Guide are applicable to all loan documentation, data and other information provided to Freddie Mac by the Seller/Servicer through the Freddie Mac Multifamily Software Applications and/or Freddie Mac Approved Third Party Applications, and that Freddie Mac will have all rights and remedies available to it under the Guide with respect to:

- A breach by the Seller/Servicer of any such warranty, or
- Any misrepresentation by the Seller/Servicer

d. No Freddie Mac liability (09/30/20)

In no event will Freddie Mac be liable to the Seller/Servicer or any other party for indirect, special, incidental, exemplary or consequential damages (including damages for loss of data or programming, loss of revenue or profits, or loss of business) arising out of, or related to, use of or inability to use the Freddie Mac Multifamily Software Applications and/or the Freddie Mac Approved Third Party Applications. Freddie Mac will have no liability to the Seller/Servicer for third-party claims made against the Seller/Servicer arising out of, or relating to, the Seller/Servicer's use of or inability to use the Freddie Mac Multifamily Software Applications and/or the Freddie Mac Approved Third Party Applications.

e. Ownership of the Freddie Mac Multifamily Software Applications (02/29/12)

The Seller/Servicer acknowledges that the Seller/Servicer has no ownership or other interest in the Freddie Mac Multifamily Software Applications, except to the extent of the rights expressly granted in the Guide.

f. Termination of the right to use the Freddie Mac Multifamily Software Applications (09/30/20)

Freddie Mac reserves the right to terminate a Seller/Servicer's use of any of the Freddie Mac Multifamily Software Applications and/or the Freddie Mac Approved Third Party Applications at any time in its sole discretion upon notice to the Seller/Servicer.

2.13 System administrator requirements (12/12/24)

a. Seller/Servicer assignment of a system administrator (06/17/21)

Prior to the Seller/Servicer's implementation of any of the Freddie Mac Multifamily Software Applications and/or the Freddie Mac Approved Third Party Applications, the Seller/Servicer must designate one or more individuals on its staff to serve as the system administrator(s) to manage access to the following:

- The Freddie Mac Multifamily Software Applications and the Freddie Mac Approved Third Party Applications, as listed in Section 2.12(a)
- Multifamily secure content on mf.freddiemac.com, including the Freddie Mac Exclusionary List

The Seller/Servicer must add, update or remove access for system administrators by submitting Form 1146, System Administrator Add/Update/Remove Request Form, following the directions found on the form.

b. System administrator responsibilities (12/12/24)

The system administrator is required to identify:

- Each Seller/Servicer employee (or vendor) who needs access to a particular Freddie Mac Multifamily Software Application, Freddie Mac Approved Third Party Application and/or Multifamily secure content on mf.freddiemac.com
- For Freddie Mac Multifamily Software Applications and Freddie Mac Approved Third Party Applications, the appropriate authority level of the employee's or vendor's access based on the employee's or vendor's roles and responsibilities

The method of identification will vary. The system administrator must:

- Enter the user's contact information in FAM, to provide access to myOptigo℠ for Investor Reporting, and the Multifamily secure content
- Enter the user's contact information in both FAM and in OUS, to provide access to OUS
- Complete the DMS New User Setup, Reactivation and Deactivation form and submit it to MF_Service_Desk@freddiemac.com, to provide access to or reactivate user access to DMS
- Enter the user's contact information in FAM, complete the Insurance Compliance Tool (ICT) User Access Request, and submit it to MF_Service_Desk@freddiemac.com, to provide

access to the ICT

- Enter user information into PRS to manage access to that software application
- Enter user information into MES to manage access to that software application
- Confirm or revoke requests for user access to CRT as appropriate
- Work with the third-party service provider to manage user access for the applicable Freddie Mac Approved Third Party Application

When an employee or vendor for a Seller/Servicer leaves the Seller/Servicer's employ or transitions to a role that no longer requires access to any Freddie Mac Multifamily Software Application or Freddie Mac Approved Third Party Application, the system administrator must, take each of the following actions in a timely manner:

- Revoke the user's access in FAM
- Revoke the user's access to OUS in OUS
- Submit the DMS New User Setup, Reactivation and Deactivation Form to MF_Service_Desk@freddiemac.com to request removal of the employee or vendor from DMS
- Submit the Insurance Compliance Tool (ICT) User Access Request to MF_Service_Desk@freddiemac.com to request removal of the employee's or vendor's access from the ICT
- Revoke the user's access information in PRS
- Revoke the user's access information in MES
- Revoke the user's access information in CRT
- Revoke the user's access information in each applicable Freddie Mac Approved Third Party Application, including Optigo Happy Inspection Application, powered by HappyCo

c. System administrator certification of valid users (09/30/20)

At least every six months, Freddie Mac will provide a user listing to the Seller/Servicer's system administrator(s), who must review the listing and certify to Freddie Mac that each user granted access to a Multifamily Software Application is a current employee of the Seller/Servicer or a vendor for the Seller/Servicer, that the user has the appropriate application access and authority level based on the user's roles and responsibilities, and that the user contact information, including the user's e-mail address, is correct. The system administrator must complete Form 1148, System User Verification and Certification, to make such certifications.

Form 1148 must be returned to Freddie Mac according to the instructions shown on the form within 15 Business Days of receipt of the request from Freddie Mac.

Any Seller/Servicer with a contract for services from a Freddie Mac Approved Third Party Application provider must obtain a user listing from such provider at least every six months. The Seller/Servicer's system administrator(s) must confirm that each user granted access to a Freddie Mac Approved Third Party Application is a current employee of the Seller/Servicer or a vendor for the Seller/Servicer, that the user has the appropriate application access and authority level based on the user's roles and responsibilities, and that the user contact information, including the user's e-mail address, is correct. Seller/Servicer's system administrator(s) must retain evidence of this review and provide such evidence to Freddie Mac within 15 Business Days of receipt of a request from Freddie Mac. Additionally, Seller/Servicer grants Freddie Mac the right to periodically request a user listing for Seller/Servicer's users from the system administrators of Freddie Mac Approved Third Party Applications.

d. Seller/Servicer officer verification and certification of system administrators (04/27/18)

At least every six months, an authorized officer of the Seller/Servicer must review and verify the record for each of its system administrators and certify the following to Freddie Mac:

- Each of the current system administrators is a current employee of or vendor for the Seller/Servicer with appropriate application access and authority level based on the system administrator's roles and responsibilities, and

- All system administrator contact information, including the system administrator's e-mail address, is correct. The officer must complete Form 1149, System Administrator Verification and Certification, to make these certifications.

  Form 1149 must be returned to Freddie Mac according to the instructions shown on the form within 15 Business Days of receipt of the request from Freddie Mac.

2.14 Electronic Signatures, Electronic Records, and data security (02/27/25)

a. Overview (05/05/17)

Freddie Mac may require or permit Seller/Servicers to conduct certain transactions with Freddie Mac electronically. Freddie Mac will identify the particular transactions that will be required or permitted to be Electronic Transactions in the Guide, in any other Purchase and Servicing Documents or by written instructions provided to each Seller/Servicer. Electronic Transactions will be subject to this section and all other applicable sections of the Guide and the Purchase and Servicing Documents.

b. Definitions (06/30/16)

As used in this section, these terms are defined as follows:

- **Computer Systems**

  All computers, servers, fax machines, other Electronic devices, hardware, web sites, Internet, private networks, telephone lines or wireless communications, together with software applications, security measures, proprietary coding, interfaces and/or connectivity used to create, present, sign, transfer, transmit, send, submit, deliver,

receive, retrieve, maintain, and/or store Records, Electronic Records or Electronic Signatures in order to engage in and/or conduct Electronic Transactions

- **Computer Contagion**

  Any computer viruses, time bombs, trojan horses, worms, trapdoors or other harmful or malicious computer information, commands, codes or programs

- **Electronic**

  Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities, as defined in the UETA and/or E-SIGN

- **Electronic Record**

  A Record created, generated, sent, communicated, received, or stored by Electronic means, as defined in the UETA and/or E-SIGN. An Electronic Record includes, but is not limited to the following:

  - A facsimile ("fax") machine copy of a Record
  - A scanned copy of a Record
  - A paper Record converted into an Electronic Record
  - An e-mail
  - Electronic information communicated or transmitted using Electronic means permitted or required by Freddie Mac

- **E-SIGN**

  The federal Electronic Signatures in Global and National Commerce Act of 2000 (15 U.S. Code, Chapter 96)

- **Electronic Signature**

  An Electronic sound, symbol or process attached to, or logically associated with, a contract or other Record and executed or adopted by a person with the intent to sign the Record, as defined in the UETA and/or E-SIGN

- **Electronic Transaction**

  An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs, using Electronic means, as defined in the UETA and/or E-SIGN

- **Host**

  Any third party selected by the Seller/Servicer or Freddie Mac to act as a web site host

- **ISP**

  Internet service provider or other method of being connected to the Internet

- **Record**

  Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form as defined in the UETA and/or E-SIGN. A Record may be a paper or an Electronic document

- **UETA**

  The Uniform Electronic Transactions Act of 1999, promulgated by the U.S. Uniform Law Commission for consideration and enactment by the States. Reference to the UETA herein means the UETA as promulgated by the U.S. Uniform Law Commission or the UETA as enacted by an applicable State

c. Scope of Electronic Transactions and Electronic Signatures (05/05/17)

Electronic Transactions and Electronic Signatures that are not expressly required or permitted by Freddie Mac pursuant to the Guide, the Commitment, the early rate-lock application or another agreement are prohibited.

d. Security standards (06/13/24)

1. Minimum standards

Freddie Mac may, in its sole discretion and from time to time, without limiting the Seller/Servicer's liability set forth in this section, establish minimum security standards that the Seller/Servicer must comply with in order to:

1. Protect and safeguard the Seller/Servicer's Electronic Signature from loss, theft or unauthorized disclosure or use; and

2. Prevent the infiltration and infection of the Seller/Servicer's or Freddie Mac's Computer Systems by a Computer Contagion.

2. Restricted access from foreign countries or regions

Notwithstanding any other provision in the Guide to the contrary, Freddie Mac may utilize traffic filtering or block or otherwise restrict the access of Seller/Servicers, their third parties and/or their respective authorized users from certain countries or regions outside the United States. This may include, but is not limited to, blocking access from countries or regions implicated by sanctions or other restrictions imposed by the Office of Foreign Assets Control ("OFAC"). Freddie Mac shall have no liability to Seller/Servicers, their third parties or any other party as a result of imposing or effecting any such restrictions on access.

e. Compliance with security standards (12/12/24)

1. Minimum security standards

- The Seller/Servicer must comply with Freddie Mac's minimum security standards within the time period established by Freddie Mac
- Freddie Mac has the right to confirm the Seller/Servicer's compliance with Freddie Mac's minimum security standards
- The Seller/Servicer's compliance with the minimum security standards does not relieve the Seller/Servicer from any of its obligations set forth in this section
- The Seller/Servicer is solely responsible for adopting and maintaining security measures that are consistent with the risk associated with conducting Electronic Transactions with Freddie Mac, including any security measures that exceed any minimum security standards established by Freddie Mac

2. Notification of Security Incident

The changes to this Section 2.26(c), as announced in the December 12, 2024 Bulletin, are effective April 1, 2025.

If the Seller/Servicer knows or reasonably believes that there has been any loss, theft, unauthorized or improper disclosure or use of the Seller/Servicer's Electronic Signature, the Seller/Servicer must immediately, and in no event later than 24 hours after the Security Incident is discovered (as defined in Section 2.26(c)), notify Freddie Mac in accordance with Section 2.26(c).

3. Failure to adopt or maintain standards

The Seller/Servicer's failure to adopt and maintain appropriate security measures or to comply with any minimum security standards established by Freddie Mac may result in, among other things, termination of the Seller/Servicer's access to Computer Systems of Freddie Mac or any Freddie Mac Host.

4. Seller/Servicer responsibility

The Seller/Servicer will be fully responsible for protecting and safeguarding its Computer Systems from any and all:

a. Computer Contagions that may cause or facilitate the destruction, corruption, malfunction or appropriation of, or damage or change to, any of the Seller/Servicer's, Freddie Mac's and/or any Freddie Mac Host's Computer Systems; and

b. Computer Contagions that enable unauthorized access to the Seller/Servicer's, Freddie Mac's and/or any Freddie Mac Host's Computer Systems.

f. Seller/Servicer's agreement regarding Electronic Records and Electronic Signatures (06/25/20)

1. The Seller/Servicer consents to the use of Electronic Records and/or Electronic Signatures whenever expressly required or permitted by Freddie Mac.

2. The Seller/Servicer agrees to adopt any Electronic Signature required or provided by Freddie Mac.

3. The Seller/Servicer agrees to adopt and maintain security measures sufficient to protect and safeguard its Electronic Signature from loss, theft and unauthorized or improper disclosure or use.

4. The Seller/Servicer agrees that if its Electronic Signature is attached to or logically associated with any Record transmitted or submitted to Freddie Mac, such attachment or association of its Electronic Signature will be conclusive verification that the Seller/Servicer executed and intended to be bound by the terms of the Record. In addition, such Electronic Signature will be deemed as valid as its ink counterpart on paper, and will not require the Seller/Servicer to conduct due diligence on DMS or on any signing technology embedded in a form downloaded from a Freddie Mac website, nor will it constitute any Seller/Servicer representation or warranty regarding the same.

5. Before Freddie Mac requires or permits the Seller/Servicer to send any Electronic Transaction to Freddie Mac, Freddie Mac may specify its requirements for the Seller/Servicer's Computer System and ISP, in which event the Seller/Servicer must ensure that it complies with those requirements.

6. The Seller/Servicer agrees that it is able to readily print, store and retrieve any Electronic Record transmitted by Freddie Mac to it; and the Seller/Servicer is able to transmit or submit Electronic Records to Freddie Mac.

7. The Seller/Servicer agrees that it is fully responsible for protecting and safeguarding its Computer System from all Computer Contagions that may damage Freddie Mac's or any Freddie Mac Host's Computer System.

g. Indemnification (06/30/16)

The Seller/Servicer agrees to indemnify, defend and hold Freddie Mac and any Freddie Mac Host harmless from and against any and all losses, costs, claims, actions, damages (including, but not limited to, indirect, incidental, special or consequential damages, whether foreseeable or not), liabilities, judgments, legal fees, counterclaims or defenses to which Freddie Mac and/or any Freddie Mac Host may become subject or that arise out of or that occur in connection with:

1. Any Computer Contagion; or

2. The loss, theft, unauthorized or improper disclosure or use of the Seller/Servicer's Electronic Signature; or

3. The Seller/Servicer's failure to comply with Freddie Mac's requirements in connection with conducting an Electronic Transaction with Freddie Mac; or

4. The Seller/Servicer's repudiation of the Seller/Servicer's Electronic Signature affixed to, attached to, or otherwise logically associated with a Record (or copy thereof) delivered to Freddie Mac; or

5. A breach of Seller/Servicer's representations and warranties under Section 2.14(j)(2), with respect to any Record delivered by Seller/Servicer to Freddie Mac bearing an Electronic Signature from a Borrower, Borrower Principal, guarantor, or their respective legal representatives/signatories.

h. Limit on Freddie Mac's liability (02/06/04)

Freddie Mac will not be liable for any of the following:

1. Any delay or failure in performing its obligation under an Electronic Transaction when the delay or failure is caused by an event beyond Freddie Mac's control:

   - That could not reasonably be expected to have been taken into account at the time of the Electronic Transaction, or

   - The consequences of which could not be avoided or overcome

2. The failure of its or the Seller/Servicer's ISP to timely, properly or accurately transmit any Electronic Record

3. Any indirect, incidental, special or consequential damages arising out of or relating to any Electronic Transaction

Except as set forth in items 1 through 3 above, the provisions of this Section 2.14(h) will not limit Freddie Mac's responsibility for any direct losses sustained by a Seller/Servicer as a result of a Computer Contagion explicitly and directly transmitted by Freddie Mac.

i. Method of notification (02/27/25)

Freddie Mac will provide each Seller/Servicer with at least 30 days' notice of a change regarding Electronic Signatures or Electronic Records unless Freddie Mac determines that a shorter notice period is necessary or advisable to protect Freddie Mac's interest. Freddie Mac will provide such notice in a Guide Bulletin or by written notice to the System Administrators.

j. Electronic Signatures from Borrowers (05/05/17)

1. Subject to Section 2.14(j)(2), Freddie Mac will accept Electronic Signatures of Borrowers, Borrower Principals, guarantors, or their respective legal representatives/signatories (as applicable), on all numbered Guide forms, except to the extent otherwise indicated on such form or requested by Freddie Mac.

2. If a Seller/Servicer elects to deliver to Freddie Mac a Record identified in Section 2.14(j)(1) signed with an Electronic Signature, the Seller/Servicer represents and

warrants as follows with respect to each such Record:

- The Seller/Servicer has conducted prior due diligence on all software and processes involved in producing the Borrower's Electronic Signature on such Record, and has confirmed that such software and processes create valid, enforceable and effective Electronic Signatures in compliance with E-SIGN and UETA. The due diligence and confirmation process includes having all necessary electronic systems and processes reviewed by internal or external technology and security experts and legal experts.

- The delivered Record is a valid, enforceable and effective Electronic Record, in compliance with E-SIGN and/or UETA, as applicable.

k. Electronic Signatures from third parties (06/30/16)

Freddie Mac will accept Electronic Signatures on all third-party reports submitted in connection with the underwriting of a Mortgage.

l. Electronic Signatures from Seller/Servicers (05/05/17)

Freddie Mac will accept Electronic Signatures of Seller/Servicers on the following documents:

- Commitments, early rate lock applications, Index Lock Agreements and all related Amendments, Adjustments/Modifications and Corrections

- Servicing approval requests

- All numbered Guide forms, except to the extent otherwise indicated on such form or requested by Freddie Mac

m. Governing law (06/30/16)

The law governing Electronic Transactions will be E-SIGN and/or the UETA, as enacted by an applicable State. Under no circumstances will any Electronic Transaction be governed by the Uniform Computer Information Transactions Act (UCITA), unless Freddie Mac expressly agrees in a written or Electronic amendment to the Purchase and Servicing Documents.

n. Conflict (06/30/16)

If the requirements set forth in this section conflict with requirements in other sections of the Guide, or with other Purchase and Servicing Documents, or any other written agreement between the Seller/Servicer and Freddie Mac, then the requirements in such other Guide sections, or other Purchase and Servicing Documents, or other written agreements (as applicable), will control and prevail over these requirements, but only to the extent necessary to resolve the conflict. If the Seller/Servicer believes there is any such conflict, the Seller/Servicer must contact Freddie Mac to discuss any such conflict in an effort to resolve it.

2.15 Standard of care (02/07/08)

The Seller/Servicer must perform its obligations set forth in the Guide and the Purchase and Servicing Documents with the same degree of care and diligence as it would perform in originating or servicing a loan for its own portfolio.

2.16 Payment instructions (04/30/19)

Before instructing Freddie Mac to make any payment via wire transfer, Automated Clearing House (ACH) (if applicable), check or any other electronic payment system, a Seller/Servicer must submit to Freddie Mac *Multifamily Cash Management* authorization documentation in accordance with the requirements of Section 32.12(a). Payments cannot be made if such authorization documentation is not on file with Freddie Mac and in compliance with the requirements of Section 32.12(a). For payments to be made via wire transfer, a Seller/Servicer also must comply with the requirements of Section 32.12(b).

2.17 Delivery of documents and forms (06/25/20)

This Guide contains instructions for the delivery of various documents and forms to Freddie Mac, including the delivery of the underwriting packages, final delivery packages and a number of different Servicing forms. In lieu of using the delivery instructions set forth in this Guide, any Seller/Servicer that is a user of DMS must deliver all documents and forms in accordance with the instructions provided in the training provided to the Seller/Servicer for its use of DMS.

The Seller/Servicer's delivery of any document or form to Freddie Mac using DMS will be deemed to be an Electronic Transaction under the Guide, and, as set forth in Section 2.14(f), if such Electronic Record contains Seller/Servicer's duly authorized employee's Electronic Signature or signature, or a copy or representation of such Electronic Signature or signature, the document or form will be as effective, enforceable and valid as a paper version of such document or form containing a duly authorized handwritten signature.

2.18 Freddie Mac Exclusionary List (12/12/24)

a. Purpose of the Exclusionary List (06/28/13)

Freddie Mac maintains the Freddie Mac Exclusionary List ("Exclusionary List") to protect the integrity of its Mortgage purchase and Servicing functions. The names of persons or entities with the roles stated in Section 2.18(c) whose conduct presents risks to Freddie Mac, as determined by Freddie Mac in its sole discretion, may be placed on the Exclusionary List, in which case such persons or entities are prohibited from doing business with Freddie Mac, either directly or indirectly.

b. Access to the Exclusionary List (02/15/21)

The Exclusionary List is updated at least monthly by Freddie Mac and is electronically available to authorized Seller/Servicers as a document as part of the Multifamily secure content. The Seller/Servicer must ensure that it uses only the most current version of the Exclusionary List. The Seller/Servicer may obtain access to the Multifamily secure content and the Exclusionary List by contacting its system administrator. Seller/Servicers can access

the Exclusionary List under "Quick Links" on the Originate and Underwrite and Asset Management web pages.

c. Use of the Exclusionary List (12/12/24)

The Seller/Servicer must use the Exclusionary List only for the purposes set forth in this Section 2.18(c). Except as provided in Section 2.18(f), if a party on the Exclusionary List has played one of the roles set forth in this Section with respect to the origination of a Mortgage, a Transfer of Ownership, or the underlying real estate transaction, the Mortgage is not eligible for sale to Freddie Mac or for Freddie Mac's approval of a Transfer of Ownership, as applicable. The Seller/Servicer must have written practices and procedures in place that instruct employees how to conduct searches of the Exclusionary List and how to verify and address potential positive and positive matches.

A Seller/Servicer may contact Freddie Mac via elist_confirmation@FreddieMac.com regarding:

- Assistance with verifying potential matches
- Questions about access to and content of the Exclusionary List

The Seller/Servicer must maintain evidence in the Mortgage File that the Seller/Servicer has used the Exclusionary List to screen the applicable individuals and entities in accordance with this section, including the date that the Exclusionary List was screened.

1. Screen employees and contractors of the Seller/Servicer.

The Seller/Servicer must ensure that no individual or entity whose name is on the Exclusionary List is employed by or contracted to the Seller/Servicer in connection with the origination or servicing of Freddie Mac Mortgages, including the Seller/Servicer's own officers, directors, employees, and any third parties to whom origination or Servicing functions regarding Freddie Mac Mortgages are outsourced, as more particularly set forth below.

The Seller/Servicer must screen each individual or entity that has a substantive role in the origination or Servicing of a Freddie Mac Mortgage, which includes, without limitation, any individual or entity that:

- Has a substantive role in any production or credit decision that is part of the origination or Servicing of a Freddie Mac Mortgage
- Is responsible for the receipt or remittance of funds in connection with the sale of a Mortgage to Freddie Mac
- Reports, remits or processes Mortgage payments
- Performs property inspections for Freddie Mac Properties

- Manages Custodial Accounts and/or performs custodial fund accounting for Freddie Mac Mortgages

2. Screen parties involved in the origination of the Mortgage.

A. Seller/Servicer must use the Exclusionary List to screen each applicable individual and entity in connection with the origination of a Mortgage and maintain evidence of the screening (e.g., screenshots of the searches) in the Mortgage File in accordance with the requirements set forth in the Guide and the Public Records Search Requirements. See also Section 2.28.

B. Prior to final delivery of the Mortgage to Freddie Mac, the Seller must screen each of the following and maintain evidence of the screening (e.g., screenshots of the searches) in the Mortgage File:

- Broker/correspondent
- Appraiser (the entity and any individual who signs the Appraisal)
- Title insurer (the entity which will issue the title policy)
- Closing agent (the entity and any individual responsible for escrowing any funds in connection with the origination of the Mortgage)
- Surveyor (the entity and the surveyor who signs the survey)
- Property condition consultant (the entity and engineer who signs the property condition report)
- Environmental consultant (the entity and any environmental consultant who signs the environmental report)
- Seller/Servicer's counsel (the firm and any attorney who prepares the preliminary legal issues memorandum, prepares any Loan Documents, manages the closing or provides any certification to Freddie Mac)
- Borrower's counsel (the firm and any attorney who signs a legal opinion or provides any certification to the Seller and/or to Freddie Mac)
- Guarantor's counsel (the firm and any attorney who signs a legal opinion or provides any certification to the Seller and/or to Freddie Mac)

C. In addition to the above, for a Targeted Affordable Housing Mortgage originated under a Forward Commitment, prior to final delivery of the Mortgage, the Seller must screen the Architectural Consultant (the entity, the on-site inspector and any consultant who signs the construction reports described in Section 63.1) and maintain evidence of the screening (e.g., screenshots of the searches) in the Mortgage File.

3. Screen parties involved in a Transfer of Ownership.

The Servicer must use the Exclusionary List to determine whether a person or entity whose name is on the Exclusionary List has played one of the roles set forth in this Section in the Transfer of Ownership or in the underlying real estate transaction.

A. The Servicer must use the Exclusionary List to screen each applicable individual and entity involved in the Transfer of Ownership or in the underlying real estate transaction in accordance with requirements set forth in the Guide and the Public Records Search Requirements. See also Section 2.28.

B. Prior to the closing date of the Transfer of Ownership, the Servicer must screen each of the following and maintain evidence of the screening (e.g., screenshots of the searches) in the Mortgage File, if applicable for the particular transaction:

- Appraiser (the entity and any individual who signs the Appraisal)
- Title insurer (the entity which will issue the title policy)
- Closing agent (the entity and any individual responsible for escrowing any funds in connection with the Transfer of Ownership)
- Surveyor (the entity and the surveyor who signs the survey)
- Property engineer (the entity and engineer who signs the property condition report)
- Environmental consultant (the entity and any environmental consultant who signs the environmental report)
- Seller/Servicer's counsel (the firm and any attorney who prepares the preliminary legal issues memorandum, prepares any Loan Documents, manages the closing or provides any certification to Freddie Mac)
- New Borrower's counsel
- New guarantor's counsel

4. Screen proposed new property management companies.

The Servicer must ensure that no proposed new property management company has its name on the Exclusionary List.

d. Process for placement on the Exclusionary List (06/29/18)

Freddie Mac will generally provide an individual or entity written notice of proposed placement on the Exclusionary List, along with an opportunity to submit a written response. However, Freddie Mac may determine, in its sole discretion, that circumstances require placement of the name of a person or entity on the Exclusionary List immediately, without prior written notice. Examples of grounds for placement on the Exclusionary List include:

- Fraud or possible fraud
- Misrepresentations, misstatements or omissions of facts
- Theft or misappropriation of funds
- Willful or reckless violation of statutory or regulatory requirements
- Business practices that Freddie Mac determines present risks to Freddie Mac
- Lack of business controls to ensure the integrity of the Mortgages sold to or serviced for Freddie Mac
- Evidence which demonstrates a lack of integrity or business competence
- Other grounds that in Freddie Mac's judgment may adversely affect Freddie Mac

Freddie Mac, in its sole discretion, will render a final decision regarding placement on the Exclusionary List after reviewing the response, if any, submitted by the proposed individual or entity.

e. Controls regarding use and confidentiality of the Exclusionary List (09/28/18)

The Seller/Servicer must maintain sufficient controls to meet its warranty obligations regarding the Freddie Mac Exclusionary List set forth in Section 5.9(c).

f. Waiver of Seller representations and warranties regarding Persons on the Exclusionary List (12/12/24)

Before the Origination Date of a Mortgage, a Seller may contact Freddie Mac to request a waiver of representation and warranty obligations under Section 5.2(g) with respect to the Mortgage. The Seller must make such request to the Freddie Mac Multifamily Fraud Mailbox.

As part of the request, the Seller must inform Freddie Mac of the nature and extent of the role played by the person or entity whose name is on the Exclusionary List in connection with the Mortgage and must provide other relevant information, upon request. If Freddie Mac reviews the request and subsequently elects to grant the waiver, Freddie Mac will provide the Seller with written notice of such election, in which case the Seller's warranty concerning the involvement of the specified excluded person or entity will not be applicable to the sale of the Mortgage. All other requirements of the Purchase Documents relating to the sale of the Mortgage will remain in full force and effect. Freddie Mac's election to review and its decision to purchase such a Mortgage are within its sole discretion.

g. Servicer representations and warranties regarding a Transfer of Ownership (09/28/18)

In addition to the warranty set forth in Section 5.9(c), prior to any Transfer of Ownership, the Servicer must represent and warrant that it has complied with the requirements of Section 2.18(c)(3).

h. Waiver of Servicer representations and warranties regarding the Exclusionary List (12/12/24)

The Servicer must contact Freddie Mac to request a written waiver prior to performing a function or entering into a transaction that would violate the Servicer's representation and warranty set forth in Section 5.9(c) or in Section 2.18(g) above.

The Servicer must make such request to the Freddie Mac Multifamily Fraud Mailbox.

As part of the request, the Servicer must inform Freddie Mac of the nature and extent of the role played by the person or entity whose name is on the Exclusionary List in the proposed transaction, and must provide other relevant information upon request. If Freddie Mac elects to grant the waiver, Freddie Mac will provide the Servicer with written notice of such election, in which case the warranty concerning the involvement of the specified excluded person or entity will not be applicable to such transaction. All other requirements of the Purchase Documents relating to the Servicing of the Mortgage will remain in full force and effect. Freddie Mac's decision regarding the waiver of such warranties is within its sole discretion.

i. Reporting obligations of the Seller and Servicer (12/12/24)

The Seller/Servicer must immediately report the discovery of any possible breach of its warranties regarding the Exclusionary List. The Seller/Servicer must make such report to the Freddie Mac Multifamily Fraud Mailbox.

j. Confidentiality and use of the Exclusionary List (06/29/18)

The identities of the persons and entities whose names are on the Exclusionary List are not publicly available, and the Exclusionary List is considered "Confidential Information" of Freddie Mac for purposes of Section 2.8. The Seller/Servicer must keep the Exclusionary List confidential in accordance with the terms and conditions of Section 2.8. The Seller/Servicer may use the Exclusionary List only as required in Section 2.18(c), and may not use or disclose the Exclusionary List for any other purpose without Freddie Mac's written permission.

k. Indemnification (06/29/18)

The Seller/Servicer must indemnify Freddie Mac for any loss, damage, or expense resulting from the Seller/Servicer's unauthorized use or failure to maintain the confidentiality of the Exclusionary List or information contained on the Exclusionary List.

l. Remedies (10/07/11)

Freddie Mac's remedies for a breach of the warranties, obligations or requirements of the Seller/Servicer regarding the Exclusionary List include all remedies available to Freddie Mac under the Purchase Documents, including suspension or termination of the Seller or Servicer, and repurchase of the Mortgage.

2.19 Compliance and regulatory risk management (12/12/24)

The changes to this Section 2.19, as announced in the June 13, 2024 Bulletin, are effective January 1, 2025.

a. Policies and procedures (01/01/25)

The changes to this Section 2.19(a), as announced in the June 13, 2024 Bulletin, are effective January 1, 2025.

Each Seller/Servicer must adopt, maintain and administer written policies and procedures that address doing business in compliance with:

- Applicable laws, regulations and orders, including the fair lending and consumer protection laws and regulations listed in Section 5.7(a); and
- Freddie Mac requirements, including origination, underwriting, Servicing, asset management and investor reporting of multifamily Mortgages and Properties

Seller/Servicers must make their policies and procedures available to Freddie Mac upon request.

1. Training

Seller/Servicers must establish compliance training implementing the policies and procedures and a regular training schedule for staff.

The compliance training must be reviewed, and if applicable, updated at least annually to ensure it includes current, complete and accurate information for compliance with Freddie Mac requirements and applicable laws and regulations.

2. Monitoring

Seller/Servicers must review and assess at least annually the adequacy of their policies and procedures to ensure compliance with applicable laws and regulations and the Guide and their other Purchase and Servicing Documents.

3. Non-compliance

Seller/Servicers must notify Freddie Mac *Multifamily Counterparty Risk & Compliance* via email at Multifamily_Eligibility@freddiemac.com within five Business Days of the Seller/Servicer becoming aware of any non-compliant or potential non-compliant activity regarding any applicable law or Freddie Mac requirement that is conducted, or may be conducted, by or on behalf of the Seller/Servicer.

b. Chief Compliance Officer (01/01/25)

The changes to this Section 2.19(b), as announced in the June 13, 2024 Bulletin, are effective January 1, 2025.

Each Seller/Servicer must designate one person as its Chief Compliance Officer (CCO). The CCO is responsible for monitoring, overseeing and managing compliance and regulatory risk for their organization.

The CCO is not required to be an officer of the Seller/Servicer. Additionally and optionally, Seller/Servicers may designate a Deputy CCO as a backup to the CCO. Designation of new CCOs or optional Deputy CCOs, or any changes to these roles, must be reported to Freddie Mac via Form 1107M (Multifamily Seller/Servicer Change Notification) within 30 calendar days.

The CCO will receive compliance communications and requests for information from Freddie Mac regarding:

- Fraud and other Suspicious Activity (see Section 2.19(c) below)
- Business continuity and recovery (see Section 2.20)
- Vendor risk management (see Section 2.26)
- Data security (see Section 2.26)
- Other compliance and regulatory matters (including Section 2.19(a) above (effective 01/01/25))

The CCO should contact Freddie Mac *Multifamily Counterparty Risk & Compliance* regarding any issues, comments or questions on any of these matters.

c. Prevention, detection and reporting of fraud and other Suspicious Activity; Restricted Vendor List (12/12/24)

1. Each Seller/Servicer must have specific prevention, detection and reporting practices and procedures in place to address fraud and other Suspicious Activity in all areas in connection with originating and selling a Mortgage to Freddie Mac and Servicing the Mortgage. Each Seller/Servicer must take the following minimum steps:

   - Comply with Section 2.18 regarding screening through Freddie Mac's Exclusionary List

   - Comply with all other provisions of the Guide relating to the prevention, detection and reporting of fraud and other Suspicious Activity. (See Chapter 7 for additional information relating to Seller/Servicer's other responsibilities with respect to the prevention, detection and reporting of fraud and other Suspicious Activity.)

2. It is also important for Seller/Servicers to know the parties with whom they do business. Each Seller/Servicer must approve, evaluate, and monitor appraisers and any third party or vendor to whom functions relating to origination or Servicing a Mortgage or REO are outsourced or assigned, and must consult the Multifamily Restricted Vendor List for each such vendor. (See Sections 29.1(c), 29SBL.1(c), 60.4(c), 61.17(e) and 62.8(e)). The Multifamily Restricted Vendor List is made available to Seller/Servicers at mf.freddiemac.com for the sole purpose of ensuring that an unacceptable third party or vendor does not perform services in connection with Multifamily Mortgage transactions and will constitute "Confidential Information" as defined in Section 2.8.

   Freddie Mac's acceptance of the engagement of any specific third-party or vendor may be subject to such additional terms and conditions as Freddie Mac deems necessary, reasonable, or appropriate in Freddie Mac's sole discretion. When applicable, Freddie

Mac identifies these third-parties and vendors as Third-Party Vendors on the "Vendors With Conditions List," which is attached as a schedule to the Multifamily Restricted Vendor List. These parties may continue to be engaged by Borrowers or Seller/Servicers but will be subject to the additional conditions described in the Vendors With Conditions List.

2.20 Business continuity and recovery (12/12/24)

a. Business Continuity Plan (12/12/24)

The changes to this Section 2.20(a), as announced in the December 12, 2024 Bulletin, are effective April 1, 2025.

Seller/Servicers and Material Vendors that present information security risk to Freddie Mac (i.e., those that have access to Freddie Mac data or systems) must implement and maintain a business continuity and disaster recovery plan ("Business Continuity Plan") that provides for the assured and continuous delivery of core operations in the event of a disaster or an incident involving a loss of, or material impact to, any facilities and personnel deemed critical to core operations ("Business Disruption"). The Business Continuity Plan must include:

- Documentation that the Business Continuity Plan can sustain the Seller/Servicer's core operations through an event involving total loss of any facilities and personnel deemed critical to core operations
- Defined recovery time objectives and a strategy for meeting those objectives
- Documentation that the Business Continuity Plan has in place backup sites with the ability to recover all core operations if a Business Disruption prevents operations at any Seller/Servicer facility
- Geographically dispersed work areas and resources available in the event of a regional disruption
- Documented procedures for crisis management, plan invocation and activation of recovery sites
- Identification of all mission-critical systems, external dependencies, network diversity, vital records, personnel and the provisions in place to ensure their continued availability
- Standards and controls that are appropriate for customers participating in the critical financial services markets

The Business Continuity Plan must be reviewed and updated at least annually.

Additionally, at least annually, the Servicer must test its Business Continuity Plan and retain evidence of the test results. The Seller/Servicer must also provide a copy of the Business Continuity Plan and test results to Freddie Mac upon request.

b. Business Continuity Plan training (12/12/24)

The changes to this Section 2.20(b), as announced in the December 12, 2024 Bulletin, are effective April 1, 2025.

Seller/Servicers must require Business Continuity Plan training that is current in substance and reflects up-to-date continuity threats and restoration strategies which are consistent with industry best practices.

At a minimum, the training must provide details on roles and responsibilities for all users that are involved in executing the Business Continuity Plan, and in protecting Freddie Mac confidential information, potentially sensitive personal information and systems.

c. Business Disruption notification requirements (12/12/24)

In the event of a Business Disruption, the Seller/Servicer must follow the requirements in the table below.

If, at any time during the investigation of the Business Disruption, there is reason to believe that there has been a Security Incident, as defined in Section 2.26(c), the Seller/Servicer must follow the requirements in Section 2.26(c).

Business Disruption notification requirements	
The Seller/Servicer must...	
1.	Immediately, and in no event later than 24 hours after the Business Disruption is discovered notify Freddie Mac of the Business Disruption via email at multifamily_eligibility@freddiemac.com and:
1a	Provide the name, phone number and email address of the contact leading the Business Disruption investigation
1b.	Promptly investigate, correct and/or mitigate the Business Disruption at the Seller/Servicer's expense, including by identifying Freddie Mac information affected by the Business Disruption and preventing the continuation and recurrence of the Business Disruption
1c.	Provide Freddie Mac with such information as Freddie Mac may reasonably request to evaluate the effect of the Business Disruption on Freddie Mac and Freddie Mac's operations
1d.	Provide Freddie Mac via email at multifamily_eligibility@freddiemac.com with all details of the Business Disruption known at that time and related internal and external investigations, including all tactics, techniques and procedures for addressing and resolving the Business Disruption

Business Disruption notification requirements	
The Seller/Servicer must...	
2.	Once known, email Freddie Mac at multifamily_eligibility@freddiemac.com with details characterizing any anticipated potential damage estimates (including reputational), what actions are being taken to protect individuals and business assets in the future, and any resulting after-action reports generated
3.	Provide to Freddie Mac updates with details on progress made since the last update until the Business Disruption is fully resolved and closed

2.21 Email communications with Seller/Servicers (07/01/14)

Freddie Mac reserves the right to send emails, including those regarding our systems, products, services, and events, to Seller/Servicer personnel at the email addresses which they use to register for Freddie Mac events, training and access to the Freddie Mac Multifamily Software Applications or other Freddie Mac systems. Seller/Servicers may adjust their email preferences at any time by visiting the Multifamily News Subscription Center on mf.freddiemac.com.

2.22 Anti-money laundering compliance (12/12/24)

Freddie Mac requires Seller/Servicers subject to the anti-money laundering provisions of the Bank Secrecy Act to establish and maintain a compliance program that ensures compliance with all applicable provisions of the Bank Secrecy Act and implementing federal regulations. Such Seller/Servicers must, as permitted by law, notify the Multifamily Fraud Investigation Unit at MF_Mortgage_Fraud_Reporting@freddiemac.com, in accordance with Section 7.2, within seven Business Days of confirmation of any instances of the Seller/Servicer's own non-compliance or compliance failure related to the anti-money laundering requirements of the Bank Secrecy Act, the Money Laundering Control Act, or Title III of the USA Patriot Act, and applicable implementing federal regulations.

2.23 Office of Foreign Assets Control (OFAC) compliance (08/15/24)

Freddie Mac requires every Seller/Servicer to establish and maintain an effective compliance program that ensures compliance with the United States Department of Treasury Office of Foreign Assets Control (OFAC) regulations. Freddie Mac will not purchase any Mortgage nor allow or approve any Transfer of Ownership under Chapters 41 or 41SBL, or approve any other Servicing-related transaction, in which any Borrower, Borrower Principal, Guarantor, Non-U.S. Equity Holder or property management company is the target of any sanctions law administered or enforced by OFAC, including those identified on the most current OFAC Specially Designated Nationals and Blocked Persons ("SDN") List or OFAC Consolidated Sanctions List. Seller/Servicer's compliance program must include written practices and procedures for conducting searches of the SDN List and the OFAC Consolidated Sanctions List including how to verify and address potential positive and positive matches on those lists.

It is the Seller/Servicer's responsibility to determine compliance with these OFAC requirements, and to verify that the names of any applicable individuals and entities do not appear on the most

current SDN List or Consolidated Sanctions List in accordance with the requirements set forth in the Guide and the Public Records Search Requirements. The Seller/Servicer must maintain evidence (including the date of the search) of the screening (e.g., screenshots of the searches) in the Mortgage File in connection with the origination of a Mortgage or any Servicing-related transaction, as applicable.

With respect to proposed Transfers of Ownership and Servicing-related transactions, Servicers should follow the procedures set forth in Section 43.28 if they determine there is a suspected or confirmed OFAC match.

2.24 Federal Housing Finance Agency (FHFA) Suspended Counterparty Program (SCP) (08/15/24)

The Federal Housing Finance Agency (FHFA) maintains a Suspended Counterparty Program List ("FHFA SCP List") and requires Freddie Mac to refrain from and/or cease conducting business with individuals and entities listed on FHFA SCP List ("Named Parties"), subject to any conditions or exclusions set forth in each Named Party's final suspension order.

Freddie Mac requires Seller/Servicers to establish and maintain written procedures to ensure they do not employ or contract with Named Parties for any purpose directly related to the origination, underwriting, or Servicing of a Freddie Mac Mortgage, subject to any conditions or exclusions set forth in each Named Party's final suspension order.

Seller/Servicers are responsible for reviewing the FHFA SCP List and related final suspension orders, which can be found on the FHFA's web site at http://www.fhfa.gov/SupervisionRegulation/LegalDocuments/Pages/SuspendedCounterpartyProgram.aspx.

Freddie Mac will not purchase any Mortgage nor allow or approve any Transfer of Ownership under Chapters 41 or 41SBL, or approve any other Servicing-related transaction, in which any Borrower, Borrower Principal or property management company is a Named Party on the FHFA SCP List, subject to any conditions and/or exclusions set forth in each Named Party's final suspension order.

It is the Seller/Servicer's responsibility to verify that each applicable individual and entity is not a Named Party on the FHFA SCP List in accordance with the requirements set forth in the Guide and the Public Records Search Requirements. The Seller/Servicer must maintain evidence (including the date the search was conducted) of the screening (e.g., screenshots of the searches) in the Mortgage File in connection with the origination of a Mortgage or any Servicing-related transaction, as applicable.

2.25 Equity Conflicts of Interest (02/22/24)

(a) An Equity Conflict of Interest occurs when:

(i) A non-executive employee of the Seller/Servicer is engaged in the origination, underwriting or Servicing of a Mortgage in which such employee or a family member of the employee has an equity interest in the applicable Borrower ("Employee-Level Owner").

Such Employee-Level Owner may hold up to 5 percent of total direct and indirect equity interest in the Borrower so long as:

- The Employee-Level Owner does not currently have, or have the ability to assume, control of the Borrower
- The property inspection and lease audit is not delegated by Freddie Mac to the Seller/Servicer
- If there are multiple Employee-Level Owners with equity interests in the same Borrower, the 5 percent threshold is applied to total combined interests per Seller/Servicer

(ii) The Seller/Servicer, an affiliate of the Seller/Servicer, an executive employee of the Seller/Servicer, or a family member of an executive employee of the Seller/Servicer ("Seller/Servicer-Level Owner") has an equity interest in the applicable Borrower.

Such Seller/Servicer-Level Owner may hold less than 25 percent of total direct and indirect interest in the Borrower so long as:

- The Seller/Servicer-Level Owner does not currently have, or have the ability to assume, control of the Borrower
- The property inspection and lease audit is not delegated by Freddie Mac to the Seller/Servicer

For purposes of Equity Conflicts of Interest, a family member is defined as a spouse, parent, child (including stepchild), grandchild (including step-grandchild), sibling or domestic partner.

(b) Equity interests held through equity investments made in third-party investment vehicles (such as REITs not managed by the Seller/Servicer, mutual funds, exchange-traded funds, index funds and SEC-registered funds) that directly or indirectly own and/or control the Property are not considered Equity Conflicts of Interest.

(c) Seller/Servicer-Level Owners of tax credit equity investments in Low-Income Housing Tax Credit (LIHTC) transactions, as a LIHTC Investor (directly or through a syndication) or as a LIHTC Syndicator, are acceptable Equity Conflicts of Interest, but must be disclosed to Freddie Mac as provided in the Guide.

(d) Equity Conflicts of Interest must be disclosed to Freddie Mac as provided in Sections 9.2, 9SBL.2, 36.18, 41.4, 41SBL.4(c), 55.2 and 55SBL.2. In addition, the Seller/Servicer must contact its Freddie Mac representative in the following instances:

(i) The ownership thresholds exceed the levels outlined above

(ii) The Employee-Level Owner or the Seller/Servicer-Level Owner of the equity interest currently has or will have the ability to assume control of the Borrower

(iii) The Employee-Level Owner or the Seller/Servicer-Level Owner of the equity interest is a Guarantor of the applicable Mortgage regardless of ownership level

(iv) The Seller/Servicer or its affiliate has an equity interest in the form of mezzanine debt, a Preferred Equity Contribution or Subordinate Financing

(v) The Seller/Servicer or its affiliate is selling a Property in which it has an equity interest and the applicable Mortgage provides acquisition financing for the Property

(vi) The individual attorney representing the Seller/Servicer in the applicable Mortgage has an equity interest in the Property or Borrower

(e) A Transfer of Servicing will be required on or prior to Freddie Mac's purchase of the Mortgage if a Seller/Servicer-Level Owner holds 25 percent or more of the total direct and indirect interest in the applicable Borrower. Transfer of Servicing is not required for LIHTC transactions with the Equity Conflicts of Interest described in Section 2.25(c).

(f) Seller/Servicer, or an affiliate of Seller/Servicer, having an equity interest in the form of a Preferred Equity investment for a non-SBL Mortgage is an acceptable Equity Conflict of Interest subject to satisfaction of the following:

(i) The Equity Conflict of Interest is disclosed to Freddie Mac as provided in the Guide

(ii) A Transfer of Servicing must occur on or prior to Freddie Mac's purchase of the Mortgage

(iii) The property inspection and lease audit may not be delegated by Freddie Mac to the Seller/Servicer

(iv) Notwithstanding the provisions of Section 60.4, neither the appraiser nor the appraisal firm may be affiliated with or related to the Seller/Servicer

(v) No other Equity Conflict of Interest is occurring

2.26 Information security (12/12/24)

The changes to this Section 2.26, as announced in the December 12, 2024 Bulletin, are effective April 1, 2025.

This section contains the minimum information security program requirements Seller/Servicers and Material Vendors that present information security risk to Freddie Mac (i.e., those that have access to Freddie Mac data or systems) must implement to reduce the impact and likelihood of unauthorized persons (or authorized persons with malicious or unlawful intentions) from gaining access to Freddie Mac's proprietary information, data and consumer personal non-public information in:

- Freddie Mac's systems
- Seller/Servicers' files, records, storage facilities and systems
- Files, records, storage facilities and systems of any third party or third-party provider that the Seller/Servicer engages to provide it with technology and/or other services

If a Seller/Servicer's regulator has established information security requirements that exceed Freddie Mac's minimum requirements, then the more rigorous requirements shall apply.

The National Institute of Standards and Technology (NIST) and the Federal Financial Institutions Examination Council (FFIEC) provide detailed guidance on their public web sites on the components of a successful information security program. Seller/Servicers are strongly encouraged to review this guidance.

Seller/Servicers should be familiar with the following terms as they relate to information security requirements:

- **Authentication**: The process in which a system verifies the identity of an individual usually based on some form of credential(s) (e.g., password/ID, token, etc.)
- **Encryption**: The process of encoding or obfuscating messages or information in such a way that only authorized parties can read it
- **Vulnerability Management:** Identification and testing of known software vulnerabilities of a system and the prioritization of remediation according to likelihood of occurrence and impact of exploitation

The Seller/Servicer must provide its information security program requirements (*e.g.*, policies and procedures), including those related to authentication, encryption and vulnerability management, and the other requirements of this Section 2.26, to Freddie Mac upon request.

a. Information security minimum requirements (12/12/24)

The changes to this Section 2.26(a), as announced in the December 12, 2024 Bulletin, are effective April 1, 2025.

(i) Information security program

Seller/Servicers and Material Vendors that present information security risk to Freddie Mac (i.e., those that have access to Freddie Mac data or systems) must define a group or identify an individual responsible for the development of information security requirements, including the adoption, implementation, maintenance and administration of written minimum security standards, policies and procedures that responsibly address critical issues including:

- User responsibilities (e.g., acceptable use)
- Ownership of information
- Baseline security practices

- Physical, administrative and technical security protection mechanisms
- Other requirements, including those described in this section

Seller/Servicers must additionally certify that Freddie Mac data is protected in accordance with their established information security policies and procedures. This certification is completed as part of the Form 16M, Annual Certification, process.

At least annually, Seller/Servicers must review and assess the adequacy of their information security policies and procedures used in connection with the selling and Servicing of Freddie Mac Mortgages to ensure compliance with the Guide and their other Purchase and Servicing Documents, and consistency with industry best practices (including as set forth by FFIEC and NIST). Seller/Servicers must make their information security program policies and procedures available to Freddie Mac upon request.

(ii) Human resources security

Seller/Servicers must meet the following human resources security requirements:

- **Pre-employment screening**: Each Seller/Servicer must conduct, or retain a qualified third party to conduct, thorough background verification checks (screening) for all candidates for employment or contractor status who will have access to Freddie Mac information

- **Confidentiality and acceptable use**: Before granting access to Freddie Mac information or systems, a Seller/Servicer must have in place written requirements that apply to its employees and, where relevant, contractors and third-party users, that require such employees, contractors, and third-party users to appropriately use and maintain the confidentiality of Freddie Mac information and systems

- **Information security awareness, education and training**: Each Seller/Servicer must provide information security awareness training to all employees of its organization, and, where relevant, contractors and other third-party users of the Seller/Servicer's information technology. The training must be current in substance, reflecting up-to-date vulnerabilities, threats and techniques and provide information on roles and responsibilities for all users in protecting information at the Seller/Servicer, along with practical ways to incorporate information security into daily routines, as well as awareness of various types of phishing campaigns and techniques.

(iii) Physical and environmental security controls

The Seller/Servicer must create and maintain:

- A physical security control program of the organization's buildings and facilities containing information systems designed to detect, monitor and prevent unauthorized persons gaining access and to respond to physical security incidents using real-time physical intrusion alarms and surveillance equipment

- Environmental controls to monitor, mitigate and protect the organization with regard to a loss of connectivity, access to, or integrity of, information and damage caused by

natural disasters or manmade incidents such as fire, earthquake, flood, hurricane, tornado or weather-related adverse conditions

(iv) Communications and operations management

The Seller/Servicer must implement technical security measures designed to monitor for, mitigate against and prevent malicious software, block unwanted spam and traffic, and protect against unauthorized use of wireless connections. Measures must include those provided in the remainder of this section and be consistent with industry best practices (*e.g.*, those set forth by FFIEC or NIST), whichever is more stringent.

(v) Data transmission and data loss prevention

The Seller/Servicer must:

- Maintain a data loss prevention/transmission protection mechanism or establish in related written policy requirements to protect the confidentiality and integrity of information exchange using technology applications or information systems, including requirements for secure data transmission across company information systems, networks and external (public and third-party) networks

- Ensure adequate and up-to-date data loss prevention (DLP) software is used and a corresponding management process is in place to scan for sensitive information stored on disk and outgoing transmissions over public communication paths as well as to restrict the transfer of data to USB and other removable media devices at the desktop level.

- Not transmit, and have measures in place to prevent transmission, to Freddie Mac system(s), through an application programming interface or otherwise, any Malicious Code. "Malicious Code" means software or firmware intended to perform an unauthorized process that may have adverse impacts on the confidentiality, integrity, or availability of an information system (including, without limitation, data in transit), such as a "virus," "time bomb," "worm," "trojan horse," or other code-based entity that infects a host; ransomware, spyware and certain forms of adware are also examples of Malicious Code.

(vi) Anti-virus program/updates

The Seller/Servicer must install anti-virus software to protect servers and end-user systems, and must keep all such software up-to-date with the latest anti-virus software and definitions.

(vii) Network security

The Seller/Servicer must:

- Implement information technology controls to block all traffic inbound from, and outbound to public networks that have not been expressly permitted by policy (i.e., "deny by default")

- Manage and restrict ports, protocols and services to only those that are required and approved for business operations

- Formally recertify and authorize firewall rules upon each significant change in infrastructure and otherwise at least annually

(viii) Mobile computing

The Seller/Servicer must have written mobile device/computing management requirements reflecting current and best practices, specifying parameters, including:

- Approved and prohibited applications

- Mechanisms to de-identify (e.g., mask or truncate) sensitive and/or confidential data

- Identity and access to management requirements

- Software updates

(ix) Wireless networks

The Seller/Servicer must control, secure and monitor wireless access points. In addition, a Seller/Servicer that offers wireless networks for network users must:

- Implement and keep up to date a strong Wireless Local Area Network (WLAN) Authentication method that meets or exceeds the current industry standard (e.g., those set forth by NIST or FFIEC) Encryption strength and technology

- Prohibit use of outdated wireless technologies such as Wired Equivalent Privacy (WEP) algorithm

- Regularly perform reviews of approved wireless networks to validate and verify authorized users and access points

- Password protect and control administrative access to the router

(x) Vulnerability management and penetration testing

The Seller/Servicer must conduct vulnerability testing on a regular basis and have a process in place to analyze and remediate identified vulnerabilities. To accomplish this, the Seller/Servicer must:

- Employ a qualified and independent third party to conduct penetration testing on system or system components at least annually. At a minimum, the executive

summary of the penetration testing report on Freddie Mac-related services and data must be made available to Freddie Mac for review upon request by Freddie Mac.

- Have written vulnerability assessment requirements that are periodically reviewed and up-to-date
- Prioritize and remediate identified vulnerabilities
- Maintain a record of all identified vulnerabilities and their status and a plan for remediation

(xi) Configuration and patch management

The Seller/Servicer must:

- Implement and maintain written patch management requirements that are periodically reviewed to stay current with standard industry practices (e.g., those set forth by NIST or FFIEC)
- Develop and execute a process for developing and maintaining secure configuration baselines (also known as hardening guides, baseline secure configurations) of infrastructure components
- Deploy an intrusion detection system (IDS) and/or an intrusion prevention system (IPS), with generated events fed into centralized systems for analysis
- Define, implement and maintain preventive controls designed to block malicious messages and attachments from entering the environment
- Designate qualified personnel responsible for performing timely software updates and patches and maintain a process for testing and installing software updates as they become available

(xii) Auditing, logging and monitoring

The Seller/Servicer must:

- Develop, implement and maintain written guidelines and requirements for the logging and monitoring of activities and action within information systems. This must include the integration with the company's enterprise log management function where applicable.
- Develop, implement and maintain written log retention and handling requirements so that logs retain relevant, useable and timely information sufficient to identify significant user access and/or system activities

The Seller/Servicer should ensure an independent security assessment of the control environment is performed not less than annually and upon the occurrence of any Security

Incident or unauthorized use or access to potentially sensitive personal information (e.g., Social Security Numbers, individual names listed with their addresses, etc.).

(xiii) Software and application development life cycle (SDLC)

If the Seller/Servicer develops applications or software that either store, access, process or transmit Freddie Mac information, the Seller/Servicer must develop, implement and maintain written SDLC requirements that include, at minimum:

- Management and separation of production and development environments that reflects contemporary best practices
- Secure coding requirements
- Open-source requirements
- Code development and security scanning pre- and post-deployment

(xiv) Treatment of personal information and Data Encryption

(i) Treatment of sensitive information

The Seller/Servicer must limit the storage, use and transmission of potentially sensitive personal information, including, without limitation, any information covered by state or federal data privacy laws, to an as needed basis. The Seller/Servicer must develop and execute a process for de-identifying sensitive personal data (e.g., masking or truncating the data) that is stored in a system. The data must be de-identified such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify the individual.

(ii) Data Encryption

The Seller/Servicer must:

- Provide for the protection, integrity and confidentiality of data in transit and at rest
- Use Encryption during transmission and at rest for any potentially sensitive personal information
- Deploy cryptography standards that meet or exceed the then current industry standard (*e.g.*, those set forth by NIST or FFIEC) Encryption strength and technology
- Prohibit use of outdated and unsupported technologies
- Generate, exchange, store, use, replace and delete cryptographic keys in a timely manner to prevent unauthorized access to those keys

- Use Encryption mechanisms on portable end-user devices to protect data, including potentially sensitive personal information, if the hardware (e.g., laptop, mobile device) is lost or stolen

(xv) Incident management

The Seller/Servicer must:

- Develop and maintain an incident response plan with a process that applies incident response capabilities and defines the resources and management support needed.

  The plan must:

  - Be tested at a pre-defined periodic frequency, or more frequently, if prudent, given the circumstances
  - Be reviewed and updated at least annually

- Periodically test the effectiveness of the incident response capabilities:

  - Annually, unless formally activated, audit the incident response plan. The audit may be performed by (i) an internal independent function within the organization, or (ii) an external entity that is qualified to conduct such audits.
  - Evaluate lessons learned from all Security Incidents
  - Implement or identify an existing classification scale for Security Incidents to quantify the severity of the Security Incident
  - Have documented action plans for remediation of Security Incidents having high severity ratings

b. Access control (12/12/24)

The changes to this Section 2.26(b), as announced in the December 12, 2024 Bulletin, are effective April 1, 2025.

(i) Access management policy

As part of its information security program, a Seller/Servicer must:

- Establish an access management policy that includes a process for granting and removing system access, requirements for Authentication and rules of behavior
- Define remote access requirements including acceptable use, approvals and recertification processes
- Develop and apply an account lock-out threshold that determines the number of failed login attempts that will cause an account to be locked out until it is reset and/or a

number of specified minutes has passed in conjunction with an account lock-out duration setting

- Define access and Authentication requirements for system administrators, including:
  - Enforce access control methods that limit access to systems, physical or virtual resources and grant access to users on a need to know basis. Access to potentially sensitive personal information must be limited to only those that must use it to perform their work.
  - Define and enforce requirements for multi-factor authentication where applicable (privileged sessions, remote connectivity, applications housing personal information, etc.)
  - Manage Seller/Servicer user accounts for Freddie Mac systems in accordance with the Guide and its applicable Purchase and Servicing Documents. Seller/Servicers must monitor for users who transfer roles or are terminated and no longer need access to their accounts as required in Section 2.13.

(ii) Granting, removing and reviewing access

Seller/Servicers must maintain written procedures for its systems for:

- Approval of access requests
- Removal of access upon employee/contractor terminations and transfers
- Analysis of account user access, inactivity and subsequent removal of access that is no longer needed for employees/contractors
- Periodic review of all user access privileges and certify access according to the principle of least privilege
- Prohibit or prevent using the same service account identifiers and passwords in both production and non-production environments

Seller/Servicers must designate one or more individuals on its staff to serve as the system administrator(s) to manage access to Freddie Mac systems in accordance with the requirements of Section 2.13.

(iii) Authentication requirements and guidelines

Seller/Servicers must require employees to authenticate or prove their identity to the system through a private, protected method or process which includes:

- User identification codes
- Passwords
- Personal identification numbers

- A smart card and/or a token device

If passwords are used, the authentication policy must mandate minimum guidelines for password complexity, reuse timelines and password change timelines, and storage of passwords outside of secured password safes.

(iv) Asset management

Seller/Servicers must maintain an inventory management system to track physical and software assets, such as end-user technology, servers, network devices, and corresponding asset ownership. The inventory management system must be reconciled to actual inventory on a periodic basis to verify all assets are included.

Documented procedures must be in place detailing guidelines and requirements for tracking the removal of assets from a facility.

(v) Cloud computing

When a Seller/Servicer consumes or provides cloud services that store, process, access or transmit Freddie Mac confidential information or any potentially sensitive personal information or connect to any system, the Seller/Servicer must maintain a formal cloud computing policy.

The policy must address:

- **Due diligence**: Specify appropriate due diligence responsibilities and ongoing oversight and monitoring of the cloud service providers' security
- **System vulnerabilities**: Articulate processes and responsibilities to securely configure cloud systems, provision access, and log and monitor the Freddie Mac information assets residing in or being processed in the cloud environment
- **Identity and access management**: Define roles for cloud access management, limiting account privileges, implementing multifactor authentication, frequently updating and reviewing account access, monitoring activity, and requiring privileged users to have separate usernames and passwords
- **Security controls for sensitive data**: Define responsibilities for implementing controls to safeguard sensitive data, including sensitive personal information, and limit a malicious actor's ability to exploit data during a breach

(vi) Vendor risk management

As required in Section 2.27, Seller/Servicers must implement a vendor risk management program and have formal written requirements in place for vendor risk management.

c. Compliance with Freddie Mac Security Incident requirements (12/12/24)

The changes to this Section 2.26(c), as announced in the December 12, 2024 Bulletin, are effective April 1, 2025.

The requirements of this Section 2.26(c) apply when:

- The Seller/Servicer knows or reasonably believes that there has been any unauthorized access to, or acquisition of, data or computing resources to Freddie Mac systems, Seller/Servicer systems, including any parent or subsidiary company's system, or the systems of vendors that may compromise the security, confidentiality, availability, integrity or privacy of Freddie Mac information (examples include a phishing email or malware attack, etc.) [("Security Incident")], or
- From the circumstances and available information, a reasonable information security professional could conclude that there has been a Security Incident

1. Notification to Freddie Mac

Immediately, and in no event later than 36 hours after the Security Incident is discovered, the Seller/Servicer must notify Freddie Mac of the Security Incident by completing the Freddie Mac Incident Intake Form.

If the Seller/Servicer is unable to access the form, notification may be done via email at Information_Security@freddiemac.com, Privacy_Incident_Management@freddiemac.com and MF_Data_Security_and_Privacy@freddiemac.com (ensure to include all email addresses) or by calling (571) 382-3333.

2. Obligation to investigate and remediate

The Seller/Servicer must promptly investigate, mitigate and remediate the Security Incident at the Seller/Servicer's expense, including identifying all Freddie Mac confidential information or any potentially sensitive personal information affected by the Security Incident and preventing the continuation and recurrence of the Security Incident.

3. Information to be provided to Freddie Mac

After notifying Freddie Mac and providing initial information about the Security Incident, the Seller/Servicer must continue to update Freddie Mac as the investigation progresses, and as Freddie Mac may reasonably request, with interim status updates, including new details learned and progress made since the last update, until Freddie Mac is satisfied that there has been compliance with applicable laws and the event giving rise to the Security Incident is fully resolved. remediated and closed.

All information should be sent to the location designated by Freddie Mac.

The information to be provided by the Seller/Servicer includes:

(i) Technical information

a. Related internal and external investigations

b. Risk factors

c. Causation factors

d. Technical indicators of compromise (e-mail addresses, hash values, IP addresses, malware code, vector of compromise, etc.)

e. Tactics, techniques, and procedures associated with the Security Incident

f. Details surrounding the attack methodology

g. Timing of the Security Incident

h. Technical and forensic reports, if available

i. Other information that Freddie Mac may reasonably request to assist Freddie Mac in evaluating the potential or actual effect of the Security Incident on Freddie Mac's infrastructure and impacted Borrowers or employees

j. Actions that are being taken to remediate the Security Incident and its cause, and to protect individuals, business assets, and Freddie Mac confidential information and any potentially sensitive personal information

k. Remediation actions or workarounds or corrections that resolved the Security Incident and restored service to its best quality

l. Eradication and recovery steps taken

m. Postmortem and similar after-action reports generated

n. Other details and information concerning the Security Incident

o. Final incident closure report

(ii) Freddie Mac and any potentially sensitive personal information

a. Whether, and if so the extent to which, Freddie Mac confidential information or any potentially sensitive personal information was accessed, taken, or exposed

b. The nature and details of the information accessed, taken, or exposed

c. All facts relevant to actual or potential misuse of the information, including the likelihood of misuse and, if applicable, how the information was misused

d. Whether there is any cyber or other insurance coverage for expenses related to the Security Incident

e. Potential damage estimates associated with the Security Incident

(iii) Compliance information

a. Actions that are being taken to comply with applicable laws

b. If requested by Freddie Mac, a Certificate of Compliance (in form and substance requested by Freddie Mac evidencing, among other things, that the Seller/Servicer has, with respect to the Security Incident, complied with applicable federal, State, and local data breach notification laws and regulations and all Purchase and Servicing Documents, including the Guide)

c. Copies of any communications to any impacted individuals, State and federal agencies and offices, regulators, credit reporting agencies or others

4. Compliance with laws

The Seller/Servicer must comply in a timely manner with applicable laws. Where a Security Incident creates an obligation to notify impacted individuals, the Seller/Servicer will first give Freddie Mac the opportunity to review and comment on any notification that in any way refers to or identifies Freddie Mac directly or indirectly.

The Seller/Servicer must comply with applicable laws that require notification to federal or State authorities. Promptly following a request by Freddie Mac, the Seller/Servicer will provide Freddie Mac and its designees all information and assistance needed to enable Freddie Mac to evaluate the need for, and to timely make, any notification it deems necessary or advisable concerning the Security Incident.

5. Limitation, restriction or termination of system access

Whether in connection with the actual or suspected presence of Malicious Code, a Security Incident, or otherwise, Freddie Mac reserves the right, in its sole and absolute discretion, at any time with or without notice, to limit, restrict and/or terminate a Seller/Servicer's access to any system(s), temporarily or permanently.

If, and when, Freddie Mac determines that restoring any level of system access to a Seller/Servicer is appropriate, as a condition to such access restoration, Seller/Servicer must provide to Freddie Mac upon request: (i) such assurances and information as Freddie Mac may deem necessary, in its sole and absolute discretion; and (ii) an attestation, executed by a duly authorized corporate officer, of the adequacy of any applicable containment, eradication or remediation of any vulnerability related to such Malicious Code, Security Incident, and the eradication of any threat actor from the Seller/Servicer's environment or any system or technology used by the Seller/Servicer (whether or not such system or technology is developed by the Seller/Servicer or by a third party and used by the Seller/Servicer).

Freddie Mac will have no liability to any Seller/Servicer or third party arising out of, related to, or in connection with Freddie Mac's limitation, restriction, or termination of a Seller/Servicer's access to any system(s).

2.27 Vendor risk management (10/19/23)

Seller/Servicers must implement a vendor risk management program to formally evaluate, track and measure third-party risk; to assess its impact on aspects of the organization's business; and to develop compensating controls or other forms of mitigation to safeguard and protect Freddie Mac's information, data such as sensitive personal data from unauthorized persons, malicious software or other harmful computer information, commands, codes or programs.

Seller/Servicers must have formal written vendor risk management requirements that are reviewed periodically and kept up-to date with current practices. Seller/Servicers must provide information about the use of a vendor to Freddie Mac upon request.

2.28 Public Records Searches (08/15/24)

Seller/Servicers must conduct the public records searches on applicable individuals and entities in accordance with the requirements set forth in the Guide, including in Chapters 2, 21, 29, 29SBL, 41, 41SBL, 43, 55 and 55SBL and the Public Records Search Requirements posted on mf.freddiemac.com (collectively, the "Public Records Searches") in the origination of a Mortgage or any Servicing-related transaction, as applicable.

2.29 Document retention and destruction (12/12/24)

The requirements of this Section 2.29 are effective April 1, 2025.

Seller/Servicers must have written data retention and destruction policies and procedures which contain minimum requirements to comply with applicable corporate, regulatory and legal standards. The policies and procedures must include the following:

- Identification or definition of the electronic or other information which are subject to the policies, including how to handle electronic or other information that is, or may be, subject to a legal or litigation-related hold
- A data storage, retention and destruction schedule
- Clearly defined criteria for destruction of electronic or other information, regardless of the form in which the information is stored
- Destruction methodology, including a process for logging and certifying such destruction has been completed

When electronic or other information is destroyed in accordance with Seller/Servicer's corporate policies in the ordinary course, or at Freddie Mac's direction, such information must be rendered unreadable and incapable of being re-created. Paper records must be properly and securely destroyed, and Seller/Servicer must retain evidence of destruction. Upon request,

Seller/Servicers will provide to Freddie Mac certificates of destruction or other evidence demonstrating the fact, time and manner of destruction, be it electronic, paper, hard drive or other media, which contained the destroyed information. Such certification or evidence is in addition to any other obligations that Seller/Servicer may have with respect to the destroyed information.

2.30 Use of artificial intelligence and machine learning (12/12/24)

The requirements of this Section 2.30 are effective April 1, 2025.

a. Compliance with applicable law (12/12/24)

The requirements of this Section 2.30(a) are effective April 1, 2025.

Seller/Servicers that use artificial intelligence and/or machine learning (together, "AI/ML") in connection with the origination of Mortgages sold to Freddie Mac or Servicing Mortgages on behalf of Freddie Mac must ensure compliance with applicable law and their Servicing and Purchase Documents. In addition, such use is conditioned upon:

- Seller/Servicer's development, implementation and maintenance of policies and procedures for the use of AI/ML, which must at a minimum:
  - Be communicated to appropriate personnel who have job responsibility in areas that use AI/ML; and
  - Have an owner(s) that implements, maintains and reviews the policies and procedures at least annually to ensure they comply with applicable law and consistently reflect industry best practices
- Upon request by Freddie Mac, Seller/Servicer's prompt disclosure of the types of AI/ML used, the purpose and manner for such use, safeguards to mitigate risks related to the use of AI/ML, and such other information as Freddie Mac may require

b. Indemnification (12/12/24)

The requirements of this Section 2.30(b) are effective April 1, 2025.

Seller/Servicer agrees to indemnify Freddie Mac and its directors, officers, employees, agents, successors and assigns, and to hold each harmless from and against any and all liabilities, losses, claims, actions, damages, including, but not limited to, indirect, incidental, special or consequential damages, whether foreseeable or not, judgments, costs and expenses, including reasonable attorneys' fees, arising directly or indirectly out of or relating to Seller/Servicer's use of AI/ML. Freddie Mac shall provide the Seller/Servicer with notice of any such claim after it comes to Freddie Mac's attention.