ZURICH

7 steps to Red Flags Rule compliance with modern threats in mind



Please route to:

- Dealer principal
- General manager
- F&I manager
- Sales manager
- Service manager
- Office manager

The Federal Trade Commission's Red Flags Rule requires automobile dealers to develop and implement a written Identity Theft Prevention Program designed to identify, detect, and respond to warning signs — known as "red flags" — that indicate that a customer or potential customer could be using stolen information to obtain an indirect or direct loan or lease at their dealership.

The Red Flags Rule dates back to 2008 (with enforcement starting in 2010) and technology has advanced at a historic pace since that time. Identity theft risks continue to evolve, shaped by AI, mobile-based fraud, and increasingly sophisticated social engineering.

Given the potential for significant regulatory penalties, maintaining an effective Identity Theft Prevention Program remains an important risk management priority. Our Risk Engineering team outlines the seven steps organizations should take today to strengthen their protection and stay ahead of emerging threats.

1. Understand your identity theft risks

A strong program starts with recognizing where identity theft can occur within your customer journey and operational processes. Evaluate your exposure to both traditional risks (e.g., mismatched personal data, forged IDs) and modern threats such as:

- Synthetic identity creation
- AI-generated deepfake impersonation
- SIM-swapping and mobile compromise
- AI-enabled phishing and social engineering campaigns

Review how accounts are opened, accessed and serviced to identify the most vulnerable touchpoints. Reassess risks regularly as fraud patterns continue to advance.

2. Build a comprehensive list of red flags

Your Identity Theft Prevention Program should identify the warning signs that are most relevant to your operations.

Continue to identify traditional red flags such as suspicious or altered documents, and inconsistent customer information, while also adding new indicators tied to today's threat environment. These include, but are not limited to:

- Unusual device behavior or login attempts
- Indicators of synthetic identity fraud
- Customer interactions that may involve deepfake audio or video

Ensure red flags are clearly documented and easy for staff to recognize.

3. Strengthen your detection tools and technologies

Modern threats require modern detection capabilities. Supplement manual checks with advanced tools, such as:

- AI-driven anomaly detection
- Behavioral analytics
- Multi-factor authentication (MFA)
- Biometric verification for higher-risk transactions
- Real-time threat monitoring systems

Ensure your detection controls scale with your business's complexity and test detection workflows to confirm they are effective against today's fraud techniques.

4. Establish fast, effective response procedures

Quick action can prevent an identity issue from becoming a financial or reputational loss. Define a clear set of steps staff should take when a red flag appears, such as:

- Locking or restricting account access
- Requiring immediate re-authentication using MFA
- Notifying customers of suspicious activity
- Elevating high-risk situations to trained specialists

Document all response actions for compliance and audit tracking, and be sure to review and refine your response plan regularly.

5. Invest in regular employee training

Threats evolve quickly and employees are a critical line of defense. Provide training that covers both foundational risks and modern threats, such as:

- Synthetic identities
- Deepfake-enabled fraud attempts

- Phishing-as-a-Service (PhaaS)
- Mobile-based attacks such as SIM swapping

Reinforce procedures for escalation and secure customer verification. It's also important to schedule periodic refresher training to keep awareness high.

6. Strengthen oversight of vendors and service providers

Your risk exposure extends to third parties handling sensitive data or customer accounts. Confirm any vendors you work with use strong protective controls, including:

- Multifactor Authentication (MFA)
- Encryption and tokenization
- Threat-monitoring tools that address modern fraud risks

Incorporate vendors into your identity theft risk reviews and require them to promptly report suspicious activity. Also, ensure any contracts with vendors reflect Red Flags Rule compliance.

7. Continuously update your Identity Theft Prevention Program

Identity theft tactics evolve rapidly. Your program should, too. Move from periodic updates to a continuous improvement model driven by new intelligence and threat trends. Regularly incorporate emerging risks such as:

- Synthetic identity fraud
- Deepfakes
- SIM-swapping
- Account takeover patterns
- PhaaS-based phishing
- AI-generated fraudulent documents

Strengthen your controls with:

- MFA for all critical systems
- AI-assisted monitoring
- Real-time fraud analytics
- Biometric options where appropriate

Ensure all updates reflect the FTC's requirement to adapt programs as new risks appear.

It's also vital for compliance that your Identity Theft Prevention Program is approved and implemented by your dealership's Board of Directors or, if no board exists, a designated member of the senior management team.

Penalties for violations

Failure to comply with the Red Flags Rule can lead to significant regulatory and financial consequences. The Federal Trade Commission (FTC) updates its civil penalty amounts annually to account for inflation, and recent increases reflect a much higher level of risk for non-compliance than in prior years.

Key points to understand:

- **"Knowing" violations of an FTC rule — including the Red Flags Rule — can result in civil penalties of up to $53,088 per violation.*** These penalty limits were updated in January 2025 under the Federal Civil Penalties Inflation Adjustment Act Improvements Act.
- **Penalties may also be assessed on a per-day basis for ongoing violations,** meaning financial exposure can escalate rapidly if issues are not corrected promptly. The FTC's updated penalty tables confirm that the $53,088 cap also applies to certain daily assessments.
- **State enforcement risk remains significant.** Businesses may face additional penalties under state unfair or deceptive acts and practices (UDAP) laws, including the possibility of individual claims, attorney general enforcement actions, or class-action lawsuits.

Partnering with you to strengthen Identity Theft Protection

Zurich's Risk Engineering team can help you assess your current program, identify gaps, and build a roadmap aligned with your industry, operations, and risk tolerance. Zurich also offers cybersecurity services that complement your Identity Theft Prevention Program, providing deeper insights, enhanced monitoring, and expert guidance to reduce exposure across your digital environment.

* All penalty figures are verified using the FTC's 2025 civil penalty adjustments.

Portions of this publication were taken from and used with the permission of Counselor Library, LLC, publisher of A Dealer's Guide to the Red Flags Rule by Michael A. Benoit of Hudson Cook, LLP.

For more information

For more information about Zurich's products and Risk Engineering services, contact your Zurich representative, visit www.zurichna.com/automotive or call us at 800-840-8842 ext. 7449.

Zurich

7045 College Boulevard, Overland Park, Kansas 66211-1523

800 840 8842 ext. 7449 www.zurichna.com/automotive

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute advice (particularly not legal advice). Accordingly, persons requiring advice should consult independent advisors when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. We undertake no obligation to publicly update or revise any of this information, whether to reflect new information, future developments, events or circumstances or otherwise. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

©2026 Zurich American Insurance Company

A1-P0664850-F (10/26) P1319250

ZURICH