# Financial services firms face surging identity-based cyber threats



Financial services firms are increasingly facing sophisticated identity-based cyber attacks, posing significant threats to security and trust within the industry. VentureBeat has reported that the financial services sector is grappling with exposure exceeding $3.1 billion from synthetic identity fraud, which saw a notable growth of 14.2% over the past year, while incidents involving deepfakes have surged by 3,000%. Projections indicate this trend may continue with a further increase of 50 to 60% anticipated in 2024.

Katherine Mowen, Senior Vice President of Information Security at Rate Companies (formerly Guaranteed Rate), a leading retail mortgage lender in the U.S., has provided insights on the measures the company is implementing to combat these identity-based threats. In a recent virtual discussion with VentureBeat, Mowen highlighted that “we face some of the most advanced and persistent cyber threats out there,” stressing the imperative of proactive defence mechanisms given the increasing rate of breaches in the mortgage industry.

Rate Companies processes billions of sensitive transactions daily and therefore becomes a prime target for cybercriminals. The firm is adopting innovative measures, including AI-driven threat modelling, to protect customer, employee, and partner identities. Mowen explained, “I think that what we’re doing right now is fighting AI with AI,” as the company seeks to enhance its Defence posture in light of growing threats.

Implementing a zero-trust framework is central to Rate's strategy. The company's operations adhere to the principle of “never trust, always verify,” which is crucial when validating identities and managing access to sensitive resources. By utilising advanced AI threat modelling, Rate can monitor transactions and workflows against a backdrop of a prompt response to potential threats. Mowen noted that as the average breakout time for eCrime incidents now sits at just 62 minutes, their organisation has adopted the “1-10-60” Security Operations Centre (SOC) model, which advocates for detecting threats within one minute, triaging them in ten, and containing them within sixty minutes.

With the cyclical nature of the mortgage industry requiring the scaling of staff from 6,000 to potentially 15,000, Rate sought a cybersecurity solution that accommodates rapid changes in workforce size and licensing requirements. The company has turned to CrowdStrike’s Falcon Flex licensing model, which offers streamlined integration across multiple layers of security.

The financial institution's approach to security includes strict monitoring of identities and their access levels. Mowen elaborated on the tools they selected to facilitate this: “Falcon Identity Protection gave us visibility and control to defend against these threats." Significant enhancements were made to their systems that previously yielded excessive alerts without actionable intelligence, shifting towards a more efficient model with CrowdStrike’s Falcon Complete Next-Gen managed detection and response.

Mowen's insights underscore the necessity of having a clear and measurable strategy in place to secure cloud environments, particularly given the organisation's ongoing growth through acquisitions. As firms adapt to a rapidly evolving digital landscape, the ability to integrate systems and respond to threats swiftly is paramount.

In looking ahead to 2025, Mowen highlights that identity security will continue to be a crucial concern across various industries. She stated, “Identities are considered a weak point in many tech stacks,” emphasising that attackers are continuously refining their techniques to exploit such vulnerabilities. The use of AI-driven defences, alongside established frameworks of continuous verification and least privileged access, will be essential in safeguarding assets against the evolving cyber threat landscape.

As these technologies advance, finding effective methods to automate responses and alleviate analyst workloads will be paramount for cybersecurity teams. Rate Companies’ experience demonstrates how adopting AI in conjunction with human expertise can strengthen the effectiveness of security measures, shaping a robust response to the challenges posed by increasingly sophisticated cyber threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://identityweek.net/customer-loyalty-at-stake-for-financial-institutions-due-to-rise-in-identity-based-attacks/> - Corroborates the rise in identity-based cyberattacks targeting financial institutions, including phishing, credential stuffing, and identity impersonation.
2. <https://www.biometricupdate.com/202410/report-synthetic-identity-fraud-is-growing> - Supports the growing concern of synthetic identity fraud, its impact on financial institutions, and the estimated costs associated with it.
3. <https://www.biometricupdate.com/202410/report-synthetic-identity-fraud-is-growing> - Provides details on the increasing frequency and impact of synthetic identity fraud, including the difficulty in detecting these identities.
4. <https://www.helpnetsecurity.com/2024/12/20/financial-industry-data-breaches/> - Highlights the prevalence of data breaches and ransomware attacks in the financial industry, emphasizing the need for modernized identity security.
5. <https://www.transunion.com/blog/money-2020-whats-behind-rise-synthetic-identity-fraud> - Estimates the financial impact of synthetic identity fraud and its projected growth, aligning with the trend of increasing identity-based threats.
6. <https://identityweek.net/customer-loyalty-at-stake-for-financial-institutions-due-to-rise-in-identity-based-attacks/> - Emphasizes the critical role of trust and security in maintaining customer loyalty, particularly in the face of data breaches and identity-based attacks.
7. <https://www.helpnetsecurity.com/2024/12/20/financial-industry-data-breaches/> - Discusses the challenges posed by overprovisioning third-party identities and the risks associated with mergers and acquisitions in the financial sector.
8. <https://www.biometricupdate.com/202410/report-synthetic-identity-fraud-is-growing> - Explains how synthetic identities can be incubated for months or years before being used for fraudulent activities, highlighting the complexity of detecting these threats.
9. <https://www.helpnetsecurity.com/2024/12/20/financial-industry-data-breaches/> - Underlines the importance of a unified, centralized platform for managing all identities within an organization to enhance visibility and threat detection.
10. <https://www.transunion.com/blog/money-2020-whats-behind-rise-synthetic-identity-fraud> - Provides an example of a financial institution discovering a significant portion of its accounts tied to synthetic identities, reinforcing the need for robust identity security measures.
11. <https://www.helpnetsecurity.com/2024/12/20/financial-industry-data-breaches/> - Supports the necessity of adopting a modernized, automated approach to identity security, given the escalating costs and regulatory fines associated with breaches.
12. <https://venturebeat.com/security/ai-threat-modeling-why-cisos-are-redefining-identity-centric-zero-trust-in-2025/> - Please view link - unable to able to access data