NICE Actimize

Insights Article

How the Proposed U.S. "Protecting Consumers from Payment Scams Act" Could Impact Financial Institutions' Fraud Prevention Efforts

As digital payment platforms continue to evolve, so do the fraudsters. The traditional protections under the U.S. 1978 Electronic Fund Transfer Act (EFTA), designed primarily for unauthorized transfers, are proving insufficient in the face of deception and social engineering.

Addressing this insufficiency, the proposed Protecting Consumers from Payment Scams Act, jointly introduced on August 2, 2024, by the House of Representatives and the Senate presents its own roadmap which addresses the EFTA's critical oversight by ensuring that fraudulently induced transfers receive the same level of protection as unauthorized transactions. This act highlights the urgent need to strengthen consumer protections in the face of rising digital payment fraud, building on existing laws to adapt to the complexities of modern financial scams.

By Anurag Mohapatra, NICE Actimize, SME and Sr. Product Manager

Fraudsters are increasingly resorting to authorized fraud, with growing focus on investment and romance scams. NICE Actimize's 2024 Fraud Insights report found that while the overall fraud value decreased by 26%, authorized fraud increased by 11%. Furthermore, NICE Actimize industry data shows a significant shift in domestic wire payments related to scams: a 44% increase in investment scams by value and 17% by volume and increases of 133% in romance scams by value and 50% by volume, away from purchase and impersonation fraud. These fraud typologies are often of higher value which results in increasing losses.

Key Amendments to the Electronic Fund Transfer Act

The U.S. Protecting Consumers from Payment Scams Act introduces several significant amendments to the EFTA aimed at enhancing consumer protections and ensuring greater accountability among financial institutions. These include:

- **Expanded Definitions** – The act broadens the definition of "unauthorized electronic fund transfers" to include transactions where a consumer's authorization was obtained through fraud. This expansion is crucial as it extends protections to consumers misled into authorizing a payment, ensuring they are not left to bear the financial burden.
- **Shared Liability** – One of the most significant changes introduced by the act is the concept of shared liability. Under this provision, the financial institution holding the consumer's account and the institution receiving the fraudulent transfer share responsibility for reimbursing the consumer. This encourages all parties involved to adopt more robust fraud prevention measures.
- **Enhanced Error Resolution** – The act expands the EFTA definition of an "error" to now include mistakes made by consumers due to fraudulent inducement. This ensures consumers who mistakenly authorize a fraudulent transaction due to deception can seek resolution and recover their funds through established channels.
- **Regulatory Oversight** – The act grants the U.S. Consumer Financial Protection Bureau (CFPB) the authority to issue new rules necessary to enforce these provisions. This includes setting guidelines for shared liability and ensuring that the protections adapt as fraud tactics continue to evolve.

Implications for Financial Institutions

The Protecting Consumers from Payment Scams Act introduces several new responsibilities for financial institutions, which will have significant operational and legal implications.

Operational Adjustments and Compliance Requirements: Financial institutions will need to make significant adjustments to comply with the new shared liability provisions introduced by the act. This includes enhancing fraud detection and prevention mechanisms, improving customer verification processes, and ensuring robust dispute resolution systems are in place.

One critical area of focus will be the detection and monitoring of money mules—individuals who transfer illegally acquired funds on behalf of criminals. Financial institutions that fail to stop mules moving funds through their institutions could be found liable for those transactions. This risk drives the need for incoming transaction monitoring, in addition to outgoing transaction monitoring commonly done today.

Institutions may also need to invest in staff training and system upgrades to meet the act's requirements, ensuring that all aspects of transaction monitoring and fraud prevention are effectively addressed.

Legal and Financial Risks: The introduction of shared liability increases financial institutions' legal and financial risks. Banks and payment service providers must now take even greater care in processing transactions, knowing they may bear financial responsibility for fraudulently induced transfers. Failure to comply with the act could result in regulatory penalties and reputational damage.

Strategic Partnerships and Collaboration: To mitigate these risks effectively, financial institutions may need to collaborate more closely with other stakeholders, including telecommunications companies, counterparty banks, and digital platforms. This is particularly relevant as many scams originate on social media platforms and over the phone, making it crucial for all sectors involved in digital communication and transactions to collaborate in preventing and mitigating scam activities. Cross-sector partnerships can enhance information sharing and enable more coordinated responses to emerging fraud threats and improve claims management.

U.S. Consumer Protection Legislation vs. Global Counterparts

When evaluating the effectiveness of different regulatory frameworks for combating payment scams, four key aspects stand out: Sector-specific obligations, liability for banks, enforcement and penalties, and information sharing. These aspects are critical because they collectively represent the essential components of a robust regulatory framework that ensures comprehensive consumer protection against scams.

- Sector-specific obligations – This aspect evaluates whether the regulatory framework imposes tailored obligations on different sectors (e.g., banks, telecoms, digital platforms) involved in payment processing.
- Liability for banks – This aspect looks at how the framework assigns liability to banks for fraudulent transactions and the extent of their responsibility to reimburse consumers.
- Enforcement and penalties – This aspect assesses the enforcement mechanisms in place and the penalties for non-compliance with the regulatory requirements.
- Information sharing – This aspect reviews the framework's requirements for sharing information about scams between institutions and across sectors.

Aspect	U.S. Protecting Consumers from Payment Scams Act	Australia's Proposed Scams – Mandatory Industry Codes	UK Payment Systems Regulator (PSR)	Singapore's Shared Responsibility Model
Regulatory Overview	Amends EFTA to address fraudulently induced transfers with shared liability.	A comprehensive, whole-of-ecosystem approach with mandatory scam codes across multiple sectors.	Comprehensive protections with mandatory reimbursement for APP fraud.	Emphasizes shared responsibility across financial and telecommunications sectors.
Sector-Specific Obligations	**No sector-specific obligations**	**Distinct codes for banks,** telecoms, and digital platforms with adaptable implementation strategies.	**Sector-specific charters for banks and** telecoms with voluntary commitments.	**Obligations for both banks** and telecoms, with a tiered approach to liability.
Liability for Banks	**Shared liability between financial** institutions for losses due to scams.	**Does not explicitly modify liability** for banks	**Sending and receiving banks share** responsibility for reimbursing consumers.	**Banks are the first line** of liability, followed by telecoms if banks meet their obligations.
Enforcement and Penalties	**CFPB oversees enforcement, but** there is room to enhance multi-sector oversight	**Strong enforcement with oversight by** multiple regulators and significant penalties for non-compliance.	**PSR enforces mandatory reimbursement,** with penalties for non-compliance.	**MAS enforces compliance,** with penalties tied to meeting obligations under the framework.
Information Sharing	**Encourages cooperation but lacks mandatory** information-sharing protocols.	**Mandatory information sharing across** sectors, coordinated by the National Anti-Scam Centre (NASC).	**Information sharing is part of** voluntary charters, focusing on fraud detection.	**Mandatory sharing of scam-related** data between financial institutions and telecoms.

The comparative analysis reveals that the U.S. Protecting Consumers from Payment Scams Act aligns closely with the UK's Payment Systems Regulator (PSR) by emphasizing shared liability and consumer reimbursement for fraudulently induced transfers.

The comparative analysis reveals that the U.S. Protecting Consumers from Payment Scams Act aligns closely with the UK's Payment Systems Regulator (PSR) by emphasizing shared liability and consumer reimbursement for fraudulently induced transfers.

However, the U.S. Act does not include the cross-sector provisions seen in other jurisdictions. Australia's proposed Scams – Mandatory Industry Codes provide an example of how robust scam controls can be implemented without altering existing liability rules for banks. Instead, it mandates improvements in systems, such as payee verification and enhanced transaction controls, to prevent scams. This approach focuses on proactive prevention and disruption across sectors, ensuring that each industry plays a role in combating fraud.

Meanwhile, Singapore's Shared Responsibility Model also highlights the importance of cross-sector controls involving financial institutions and telecommunications providers. This is particularly relevant as many scams originate on social media platforms, making collaboration crucial in preventing and mitigating scam activities.

Strengthening Against Scams

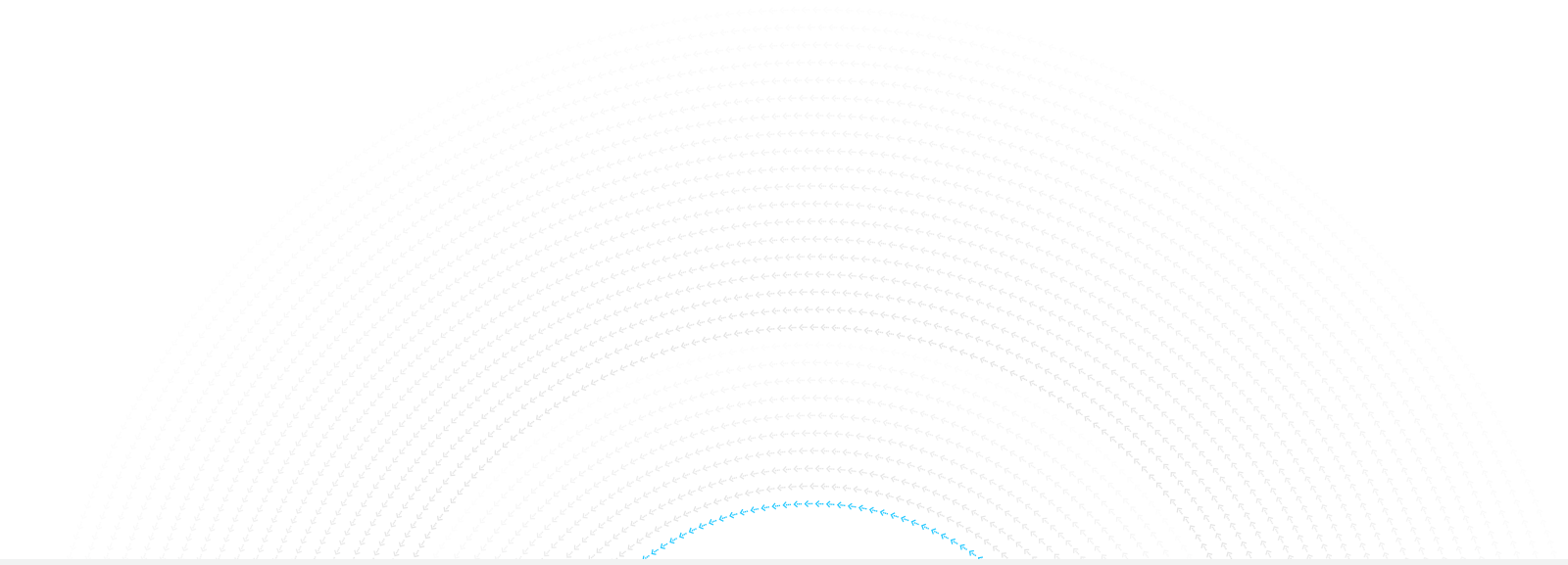
Financial institutions can take steps to protect their customers from scams that impact the bottom line, regardless of whether the proposed legislation is signed into law by U.S. Congress. These include using additional external intelligence resources to ascertain beneficiary risk, target first-party fraud, and aid in authorized fraud detection. Other options include creating multiple risk profiles to aid models and rules, including beneficiary and institution risk and the payer and payers' institution risk. as well as putting in place separate machine learning (ML) models and scoring for ATO and authorized fraud.

There are also a number of strategic and industry-facing steps that an organization can utilize. First, an FI can participate in an industry information sharing or collective intelligence initiatives that provides holistic insights beyond what the individual FI could see independently. An organization should also create strategies or policies that address each specific fraud type, such as setting up distinct step-up authentication for ATO and scams. Another approach is to use distinct processes for fraud investigations that detect first-party authorized claims and manage cases and refunds within regulatory timescales where regulated. Last, it's crucial to improve reporting capabilities to better measure scams separately from unauthorized fraud and claims fraud rates, empowering you with better control and insights.

Should the legislation pass, financial institutions should also consider the implications of liability shifts on their fraud detection program. Money mules, which previously had little financial impact on your institution, could significantly contribute to your overall fraud losses with mandatory reimbursements to counterparty institutions. When strengthening money mule detection, one key place to start is setting up fraud monitoring on incoming transactions.

Don't Wait to Start

The proposed legislation is expected to take some time to pass through the U.S. House and Senate. During that timeframe, the contents of the act could be modified. Financial institutions shouldn't wait for a passed act to start preparing their program for the potential implications. There are steps they can take today to protect their customers that will reduce scam-related fraud losses, bill or not. To learn about how you can use the latest technology to stop scams and mules, check out NICE Actimize's Scams and Mule Defense solution.



About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com