Crowe

January 2019

Regulation E Error Resolution

An article by Emily M. Morrissey, CRCM, and Niall K. Twomey, CRCM

Despite an ever-changing consumer protection regulatory environment, error resolution requirements within Regulation E of the *Electronic Fund Transfer Act* (EFTA) have not changed substantially since its passage. Consequently, some financial institutions have relaxed their approach to Regulation E compliance, risking violations, penalties, and possible restitution in addition to potential damage to the consumer base, adverse financial impact, and reputational harm.

When Regulation E was first enacted in 1978, electronic fund transfers (EFTs) were just starting to increase in number because of the growth of automated teller machines (ATMs), debit point-of-sale (POS) terminals, telephone bill-payment plans, and automated clearinghouse (ACH) transactions. Regulation E contains the standards and procedures used by financial institutions to resolve errors reported by consumers related to EFTs. Even though paper-based transactions outnumbered EFT payments in 1978, the emerging trend was clear.

Today, trillions of dollars pass electronically on a global basis through financial institutions, businesses, and individual holders via credit and debit cards, prepaid cards, and ACH payments. Because this significant rise in EFT volume has been accompanied by a significant rise in EFT error claims, regulators have been intensifying their scrutiny of error-resolution processing and regulatory compliance. Financial institutions that view Regulation E as simply a low-risk deposit regulation put their organizations at significant risk.

Error resolution definitions and requirements

In order to grasp EFTA and Regulation E requirements, it is important to understand a financial institution's error resolution responsibilities and the Federal Reserve's definition of an error. Section 1005.11 of Regulation E presents the specific procedures that financial institutions must follow when receiving an EFT error notification from a consumer. It defines an error as one or more of the following:

- An unauthorized electronic fund transfer
- An incorrect electronic fund transfer to or from the consumer's account
- The omission of an electronic fund transfer from a periodic statement
- A computational or bookkeeping error made by the financial institution relating to an electronic fund transfer
- The consumer's receipt of an incorrect amount of money from an electronic terminal
- An electronic fund transfer not identified in accordance with Section 1005.9 or Section 1005.10(a)
- The consumer's request for documentation required by Section 1005.9 or Section 1005.10(a) or for additional information or clarification concerning an electronic fund transfer, including a request the consumer makes to determine whether an error exists under paragraphs (a)(1)(i) through (vi) of this section[1]

The Federal Reserve states that consumers can provide either written or oral notice of an error. To be in compliance with Section 1005.11 error resolution procedures, financial institutions need to respond to any notice of an error that:

- Is received by the institution no later than 60 days after transmitting the periodic statement on which the error is first reflected
- Enables the institution to determine the consumer's name and account number
- Indicates why the consumer believes an error exists
- Includes, to the extent possible, the type, date, and amount of the error

Error investigation time limits and extensions

Regulation E also lays out specific timelines in which financial institutions must complete investigations into error reporting and resolution. A financial institution must complete error investigations within 10 business days of receiving notice, and the 10-business-day limit applies even if the institution required consumers to provide written notice to them. The institution might risk noncompliance if it waits to begin the investigation until after it receives written confirmation after a verbal notification. However, as long as the situation meets certain conditions, the 10-day period might extend to 20 or 45 days, and the 45-day period might extend up to 90 days, pending review.

In order to comply with regulations relating to the longer times for resolving errors under 12 CFR 1005.11(c)(3), financial institutions must disclose these time periods to consumers. All time limit extensions for investigations require that financial institutions provide an explanation of the findings and make copies of documents used in the investigation available upon request as well as notify consumers about debiting of provisional credit. Sending a written explanation of findings to the customer isn't required if the financial institution determined an error occurred. Providing the explanation in writing is only required if no error occurred. If an error occurred, a financial institution may notify the customer verbally.

The Federal Reserve outlines specific criteria related to time-limit extensions:

- **10 to 20 days.** The institution may take up to 20 days if the notice of error involves an electronic fund transfer to or from the account within 30 days after the first deposit to the account was made.
- **10 to 45 days.** The institution may take up to 45 days from receipt of a notice of error to investigate and determine whether an error occurred, provided the institution:
  - Provisionally credits the consumer's account in the amount of the alleged error
  - Informs the consumer, within two business days after the provisional crediting, of the amount and date of the provisional crediting and gives the consumer full use of the funds during the investigation
  - Corrects the error, if any, within one business day after determining that an error occurred
  - Reports the results to the consumer within three business days (in writing, if an error occurred) after completing its investigation, including, if applicable, notice that a provisional credit has been made final
- **45 to 90 days.** The institution may take up to 90 days if a notice of error involves an electronic fund transfer that:
  - Was not initiated within a state
  - Resulted from a point-of-sale debit card transaction
  - Occurred within 30 days after the first deposit to the account was made

Threat and risk mitigation

Financial institutions should acknowledge that regulators have actually increased Regulation E investigations, in part because of the continued expansion of EFTs in day-to-day transactions, but also because of the increase in cybercriminal technologies and related consumer complaints. The possibility of data breaches and fraudulent transactions is simply a fact of life for today's consumer. Well-informed consumers now proactively monitor points of personal risk such as banking transactions, credit card usage, and data exposure such as the Equifax breach, which compromised the data of more than 140 million individuals.[2]

In 2017, a record number of data breaches took place[3], and new threats such as the increased sophistication of ATM malware emerged for financial institutions and consumers. With the continued rise in cybercrime, data complexity, and widely dispersed information, financial institutions have to balance attention between banking, information technology and security, big data management, compliance and governance – and all the inherent risk associated with each of these areas – while still trying to increase market share and profitability. The development and maintenance of effective first-line monitoring systems and controls and a comprehensive approach to enterprise risk assessment are just the initial steps in mitigating Regulation E compliance issues.

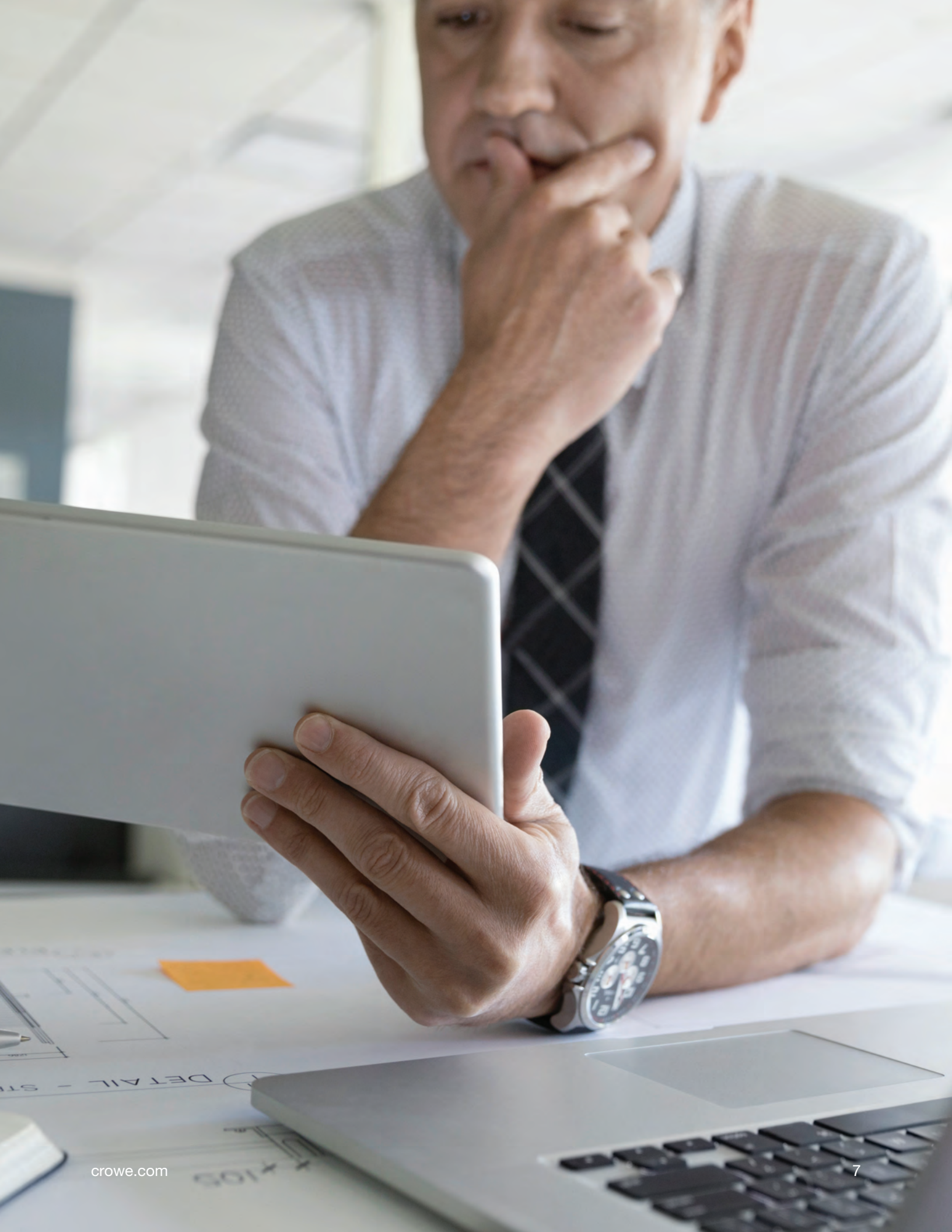
Financial institutions must also examine their internal error resolution platforms to make sure that aligned systems and departments are communicating efficiently and effectively across the enterprise. For example, dispute intake might occur outside of the error resolution platform, or different internal departments might process ACH, POS, or ATM disputes, but the related information needs to be distributed and communicated appropriately. Additionally, short, specific timelines and requirements within Regulation E mean that financial institutions need to monitor error-notification time stamps in order to comply with the law.

As a result, establishing effective control frameworks and communication strategies is critical. Poor communication among typically siloed departments such as customer service, fraud, and information security can often lead to miscommunication or lack of critical departmental communication and put the institution at risk of noncompliance. Ownership is key because internal business groups might initially rely on the compliance team for their control frameworks. However, such a strategy could lead to defective controls without a proper level of first-line collaboration. Organizations should also determine if other regulatory requirements or even outside service providers drive or affect their error resolution process, and consider what this means from a Regulation E standpoint.

Moving forward

With Regulation E violations that can reach $500,000 or 1 percent of a bank's net worth in a class action suit, the potential fiscal impact is significant.[4] Financial institutions can significantly reduce the risk of such fines by developing and implementing an effective system of internal controls and procedures related specifically to an error-resolution platform. A comprehensive, enterprisewide compliance risk assessment will not only help leaders gain a better understanding and awareness of their institutions' risk level related to Regulation E, but it could also encompass Regulation Z and other consumer compliance regulations, further protecting the organization. Additionally, performing an ongoing risk and control self-assessment (RCSA) can help an organization assess its controls, identify and prioritize risks as measured against critical business objectives, and measure the results of compliance efforts. A consistent approach to risk can improve monitoring and audit results and lead to greater efficiency.

As business strategies, data platforms, and cybercrime continue to advance in line with technology, so will the need for continued stringent checks and balances by financial institutions to stay ahead of consumer complaints and regulatory agency check-ins and examinations. Rather than simply seeking to comply with their obligations, institutions that proactively embrace their deficiencies in order to turn them into efficiencies can come out ahead – in the eyes of consumers and, ultimately, in market share.



Learn more

Emily Morrissey
+1 630 706 2089
emily.morrissey@crowe.com

Niall Twomey
Principal
+1 630 574 1806
niall.twomey@crowe.com

---

[1] 12 CFR Part 1005 (Regulation E), Section 1005.11, "Procedures for Resolving Errors," Consumer Financial Protection Bureau, https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/11/

[2] Shawn Knight, "Equifax Reveals Full Extent of Last Year's Massive Data Breach," TechSpot, May 8, 2018, https://www.techspot.com/news/74523-equifax-reveals-full-extent-last-year-massive-data.html

[3] Eva Velasquez, "2017: Another Record-Breaking Year for Data Breaches," CyberScout, Feb. 7, 2018, https://cyberscout.com/education/blog/2017-another-record-breaking-year-for-data-breaches

[4] "Consumer Compliance Handbook," Federal Reserve, Page 17, Regulation E (1/06), https://www.federalreserve.gov/boarddocs/supmanual/cch/200711/cch200711.pdf

crowe.com

RISK-19003-002B