



## **ACH Operations Bulletin #2-2025**

### **Encouraging the Use of Secure Electronic Channels for Resolving ACH Exceptions**

August 14, 2025

#### **Summary**

For decades, the business world has used unencrypted electronic mail and fax machines to resolve disputes and transmit images of documents. Related to ACH processing, such interactions and business documents often contain details necessary to resolve an exception that prevented straight-through processing of an ACH payment, or to process a request or claim regarding an ACH payment. For example, an Originating Depository Financial Institution (ODFI) might need to provide proof of a consumer's authorization for an ACH Debit at a Receiving Depository Financial Institution's (RDFI's) request, or provide a signed Letter of Indemnity to support a request for the return of an ACH Credit from an RDFI. Because of security vulnerabilities inherent in the processes associated with communicating to non-authenticated recipients, and in sending and receiving faxes or email to unintended parties, Nacha recommends the use of secure electronic channels as a best practice for sharing information and exchanging documents necessary to resolve ACH exceptions.

#### **Discussion**

Exception cases related to ACH Entries typically include sensitive data elements such as names and account numbers. The Nacha Operating Rules require ACH participants to protect the security and integrity of certain ACH data throughout its life cycle. Exception cases necessarily exist in support of the life cycle of an ACH Entry. When the data elements of an Entry are communicated outside the ACH Network in an exception case, the data elements deserve protection similar to the protection they receive when they flow through the ACH Network.

The use of unencrypted email and fax is not inherently secure. Sending a fax or an email depends on the accurate entry of a fax number, address, or similar identifier to transmit a document image to an intended recipient. An error in entering this information can send a document not simply to an unintended recipient, but to a recipient in an unrelated environment that is not subject to data security requirements and that might mishandle or even exploit the information it receives. Additionally, physical facsimile machines often stand unattended in a shared workspace where an incoming document might be retrieved by someone other than the intended recipient who is working on a particular case. Even within a secure environment, this violates the spirit of limiting access to those with a need for the information being transmitted.

## **Nacha Encourages the Use of Secure Electronic Channels**

To underscore Nacha's emphasis on using secure electronic channels for communicating sensitive information, any new categories added to the ACH Contact Registry in Nacha's Risk Management Portal—such as Exception Resolution and Information Security contacts—will not capture fax numbers. The ability to capture, transmit, and store information in an electronic environment has advanced considerably since the advent of the fax machine. Access to secure forms of electronic communication has become so prevalent as to make the use of an inherently unsecure method of communication unnecessary. For this reason, Nacha strongly recommends that all Non-Consumer Originators, Participating DFIs, Third-Party Service Providers, and Third-Party Senders abandon the use of unencrypted electronic mail and faxes, and use only a secure electronic channel when exchanging information and documents to resolve ACH Exceptions.

###