



# Retail Payments Office

of the Federal Reserve System

1000 Peachtree Street, N.E. Atlanta, GA 30309-4470

Dear CEO:

As an ACH operator, our highest priority is making the ACH system as safe and secure as possible. We are writing all financial institutions to ask for your help in this effort, with specific emphasis on risk management practices.

As you know, in recent years risk management, especially involving non-recurring debit ACH originations, has become a concern for many participants in the ACH system. Both of the ACH operators working with NACHA, have increased efforts to identify and monitor potential risk situations, including the development of risk management tools. In addition, law enforcement officials and regulators have begun to look closely at best practices for preventing fraud and minimizing risk in the ACH.

Our experience as an ACH operator teaches us that the originating bank (ODFI) is the key to effective risk management. The ODFI knows its originators and is the only ACH participant that is in a position to understand the originator's business and the level of risk that an originator's business poses.

We are asking your institution to take a careful look at your ACH risk management practices, especially your risk management practices regarding ACH debit origination by third-party merchant processors. We are enclosing a letter from NACHA that sets forth recent lessons learned regarding the risks of debit origination and how those lessons can be applied to appropriate risk management for ODFIs. While each ODFI is in the best position to understand and manage its own risks, we believe that NACHA's letter raises important issues and every ODFI should take this occasion to review its own risk management policies and procedures.

If you have questions regarding the ACH risk management tools that we can provide to you, or questions or concerns about your institution's ACH risk management policies or procedures, please do not hesitate to contact your local FedACH Sales Specialist.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard Oliver", written over a light gray rectangular background.

Richard Oliver  
Executive Vice President

Enclosure

cc: ACH Operations Contact

To: Chief Executive Officer

Subject: ACH Risk Management

As the administrator of the ACH payments system, we are calling on you to renew your institution's commitment to risk management and best practices in originating ACH payments for your customers. National banking regulators are also requesting national banks focus special attention on ACH risk management.<sup>1</sup> Attached is a series of six principles that should be addressed by all financial institutions and particularly those engaged in originating ACH payments for corporate customers.

The negative impact of a recent episode across payment systems - credit card, debit card, ACH, and checks - highlights the need for financial institutions to pay special attention to risky payment practices.

### **12DAILYPRO AND STORMPAY**

From late 2005 through early 2006, a web site called 12DailyPro operated as an "autosurf" high-yield investment. Investors transferred funds to 12DailyPro, viewed a specified number of web-based advertisements, and received payouts from 12DailyPro for their activity. Investors transferred funds to and from 12DailyPro through StormPay, a private Internet-based company operating a proprietary stored value system. Investors funded their StormPay accounts through banking payment instruments – credit cards, debit cards, ACH debits, and checks.

In early- to mid-February 2006 there was a sharp rise in the number of ACH debits returned as unauthorized in which StormPay was the Originator. On February 27, 2006, the Securities and Exchange Commission (SEC) charged 12DailyPro with operating a Ponzi scheme, and froze its assets including its StormPay account. With investors unable to withdraw funds out of the StormPay system, many availed themselves of payments system rules to claim to their financial institutions that the original funding transactions by credit card, debit card or ACH were unauthorized.

### **LESSONS FOR ODFIS**

The StormPay episode highlights several lessons for financial institutions that originate ACH payments on behalf of corporate customers (ODFIs):

#### ***Lesson 1: Know Your Customer, Know the Rules***

It is critical for ODFIs to know their customers, and in the origination of large numbers of ACH debit entries, it may be important to know the customer's customer. One of StormPay's customers was operating a high-risk business. StormPay<sup>2</sup> had previously been cited for operating a Ponzi scheme by the State of Tennessee Division of Securities. It is also critically important for an ODFI to understand the risks that accompany the origination of debit entries. The potential consequences of breaching the warranties in NACHA's rules can be catastrophic for an ODFI, and the length of time an ODFI's warranties exist under state law means that the financial risk to an ODFI lives on long after the ODFI originates unauthorized entries.

---

<sup>1</sup> See, e.g., Office of the Comptroller of the Currency; OCC Bulletin 2006-39; "Automated Clearing House Activities: Risk Management Guidance," dated September 1, 2006. The bulletin can be accessed online at: <http://www.occ.gov/ftp/bulletin/2006-39.pdf>.

<sup>2</sup> See Tennessee Securities Division vs. Tymglobal, Inc., StormPay, Inc., and John R. McConnell, Jr. File No. 03-020, August 7, 2003

### ***Lesson 2: ODFIs Should Monitor Returns***

StormPay had an excessive return rate. Over a 60-day period, StormPay originated through a single ODFI over \$40 million in ACH debits, with over \$20 million of debits returned unpaid. A high return rate is an important indication of a problem for an ODFI that originates large volumes of debit entries. This indication of a potentially serious problem is useful only if the ODFI monitors return rates.

### ***Lesson 3: Risk Management Is a Full-Time Job***

A sudden change in the business of an ODFI's customer could quickly move the ODFI into a high-risk situation. For example, StormPay originated ACH debits for a year with relatively low return rates. When 12DailyPro became a customer of StormPay, the return rate increased dramatically. A significant change in the ACH originations of an originator means that the ODFI needs to pay attention.

### ***Lesson 4: All Risk Exposure Must Be Considered***

ODFIs must understand and manage their exposure over the entire 60-day return window that is fundamental to the ACH Network. Many ODFIs set and manage daily exposure limits with their Originators, but few factor in exposure over the entire cycle in which a consumer ACH debit can be returned unpaid.

The 12DailyPro-StormPay episode highlights the extended risk to ODFIs for unauthorized debits introduced into the ACH Network. The ODFI warrants that all debit transactions that it sends into the ACH Network are authorized. This warranty extends for at least two years and could be even longer under individual state laws. The receiving depository financial institution (RDFI) has a legal claim on funds obtained without authorization. Furthermore, under ACH Network Rules, the RDFI may initiate an uncontestable return against the ODFI up to 60 days from settlement of the original transaction if its customer signs a written statement under penalty of perjury.

The pursuit of prudent risk management practices, such as those attached, will allow you to take advantage of the opportunities afforded by today's ACH Network while still protecting your financial and reputational interests. For additional information on managing the risks associated with ACH debits, please familiarize yourself with the risk management tools available from your ACH Operator, and the resources and education provided by NACHA and your Regional Payments Association.

Sincerely,

NACHA – The Electronic Payments Association

Attachment:  
Essential Risk Management Principles for ACH Origination

# Essential Risk Management Principles for ACH Origination

Risks to an ODFI in ACH origination can be managed using methods that are familiar to all bankers. Before permitting a customer to originate ACH debit entries, an ODFI should take adequate steps to know the customer and the customer's business. In accordance with the *NACHA Operating Rules*, the ODFI should determine the credit-worthiness of the customer. Familiarity with the customer's business practices is an important protection against losses that the institution might incur if the customer violates applicable rules.

The pursuit of prudent risk management practices, such as those outlined below, will allow ODFIs to take advantage of the opportunities afforded by today's ACH Network while still protecting their financial interests. For additional information on managing the risks associated with ACH debits, ODFIs should familiarize themselves with the risk management tools available from the ACH Operators, and other providers, as well as the resources and education provided by NACHA and the Regional Payments Association.

## 1. Balance sales culture with risk management. Key steps include:

- Ensure ACH risk exposure is measured, monitored and reported. Also, monitor ACH returns. If your institution is receiving a significant number of ACH return items that relate to debits originated by one of your customers, there could be serious trouble brewing. Your daily settlement advices from your ACH Operator will itemize the dollar volume of ACH returns being charged to your account and provide insights as to the need for further investigation of individual originators.
- Ensure account officers and credit administrators fully understand credit risk in ACH origination, including the potential maximum credit exposure vs. daily and multi-day limits (and for consumer ACH debits, this includes the extended return window).
- Ensure origination customers understand and fully comply with reasonable ACH risk management requirements and the NACHA Operating Rules.
- Increase credit risk and credit policy awareness among operations staff while ensuring communication and accountability with credit administration, risk management and audit staff.

## 2. Ensure that your contracts with customers that originate ACH debit items specifically require the customer to follow the NACHA Operating Rules:

- Become knowledgeable about the NACHA Operating Rules and include your responsibilities and liabilities for payments settling against your account.
- Ensure that origination and processing agreements protect your institution and allow for prompt action in case requirements are not met.
- Understand that regulators, law-enforcement authorities, and payment-system authorities expect ODFIs to thoroughly understand their customers' business and the nature of the transactions that these ODFIs will be entering into the system on behalf of their customers. Most particularly, where an ODFI's customer is a third party originating ACH entries on behalf of others, regulators may expect the ODFI to obtain certain information identifying the customers whose transactions will be sent through the ODFI so that the ODFI can do risk-management due diligence.

## 3. Scrutinize third-party processors and third-party senders on an ongoing basis:

- Make sure the party that actually obtains the funds from ACH debit entries originated through your institution has followed all of the rules.

- You may need to require your customer to disclose the terms and conditions under which it does business with its customers. Once again, credit-worthiness checks are effective tools and upstanding companies will be happy to assist and be scrutinized.
4. Be careful before you allow any customer to use your institution's electronic access capabilities to an ACH Operator ("direct access"). Your institution is responsible for settling all ACH transactions that are originated using your routing and transit number:
    - Use the "Know Your Customer" principle to guide the decision to hand your customer the keys to your institution's clearing account.
    - In addition to performing due diligence prior to giving any customer direct access to an Operator, it is critically important to monitor the account activity of these customers on a regular basis.
  5. Consider the possibility of establishing a "return reserve" requirement for customers that originate certain types of ACH debits through your institution. Bad actors are likely to respond to such a requirement by taking their dishonest enterprises elsewhere.
  6. Assessing risk and the criticality of business continuity planning and data security are a high sense of priority. If your institution is working with third-parties, ensure proper control over your relationship in these areas.

We invite you to familiarize yourself with your ACH Operator's risk management information and related offerings at <http://www.frbservices.org/Retail/fedachRisk.html> for the Federal Reserve Banks or <http://www.epaynetwork.com/cms/services/processing/value/risk/001478.php> for EPN. For additional information, visit NACHA online at [www.nacha.org](http://www.nacha.org) or contact your Regional Payments Association.