

ACH Fraud

By Steven Bernstein
September 2010

The following podcast is brought to you by J.P. Morgan.

Good afternoon. My name is Steve Bernstein. I'm an ACH Product Manager at J.P. Morgan. Today's subject is regarding ACH fraud and how to prevent it. We'll focus on having to make your process bulletproof within the corporate office-place. Probably no topic has been so timely in the last several years as fraud prevention, and we'll focus our thoughts around the corporate space, but also interject with other opportunities that you may have for monitoring your ongoing situation within your office-place and employing best practices with regard to your client base.

J.P. Morgan has worked hand-in-hand with AFP Payment Fraud and Control Survey of the last several years, and we've taken some of that information to heart. Some of the things I'm going to focus on today include best practices with talking to a lot of our clients in terms of employing and deploying, monitoring, and fraud prevention within their office space. The first thing that we typically focus on is the idea of an ACH debit block. Most of the respondents from the AFP fraud study have determined that they employ debit block within their corporate space. One of the challenges that our corporates have is that occasionally they do not debit block all of their accounts, but only those accounts that have the largest type of activity and the largest traffic of activity. Our strong recommendation is that every ABA and DDA that you have with all of your banking partners should be debit blocked or debit filtered. Even if you allow a government agency to debit your account, you should monitor it. In most cases where you don't allow an ACH debit to that account, have a debit block in its entirety, where you do not allow any incoming ACH debits to occur.

Invariably we hear stories from our corporate partners whereby there may have been a day where the corporation was open and the bank was closed, or vice versa, where the settlement and proof and control did not take place on a timely basis. Most corporate debits allow 24 hours for that item to be returned, and if you don't employ effective and timely proof and monitoring control, if you let that 24-hour span elapse, then you may be in a position of vulnerability. So again, we strongly recommend ACH debit blocks and/or filters on every one of your DDAs.

A recent addition to our array of services has been ACH Positive Pay, also known as ACH Transaction Review. We also recommend that this be deployed through our Payables Web Services portal, whereby the day after a transaction report is emailed to the designated practitioner to identify any ACH debits that have occurred and allow you the opportunity to return those unauthorized transactions within that same day. Now, this type of process requires additional support and vigilance on behalf of the corporate practitioner. ACH Positive Pay is an attribute that many of our corporate practitioners have requested over years, but let it be said that unlike an ACH debit block or debit filter, which is a rote type of service whereby the direction to either accept or not to accept given transactions based on a dollar value, based on allowing any transactions at all, or by allowing certain practitioners to debit your account, ACH Positive Pay or Transaction Review requires an active participation by the corporate practitioner. So you have both levels of capability within J.P. Morgan: one that is a rote service, which is ACH Debit Block and/or Debit Filter, or one that requires active participation, which is ACH Positive Pay.

Another service that many of our clients have found an interest in is something known as a UPIC. A UPIC is a universal payment identification code, and this is where the EPN — the electronic payment network — allows any incoming corporate credit transaction to utilize a UPIC. So what happens here is, simply put, the EPN stores the actual ABA and account number of a corporate practitioner. A UPIC is in fact a code or in effect a pseudo-number that the corporate practitioner can designate to their counterparties to utilize in lieu of their actual account. So if that party is paying the corporation, then that party or counterparty will use the UPIC number instead of the corporate's actual account. In this way the corporation never has to provide or list their actual account information, so that party remits the payment to our

corporate partner with that UPIC number in lieu of their actual account.

UPICs are becoming increasingly desirable for those that may publish this information on their website or increasingly looks for their counterparties to pay them electronically instead of by check, but does not want to offer up their actual account number. It also must be said that under no circumstances should a corporation ever put their account number on a website. Unfortunately, we know of many corporates that do in fact put their ABA and account number on their website, allowing that party to potentially perform or attempt fraud on that activity for that corporation. We can't stress enough that the more you limit access or knowledge of your account, the better chance you have of combating and bulletproofing your process to prevent against fraud.

So far we've reviewed ACH Debit Block and ACH Debit Filter. We've talked about ACH Positive Pay or Transaction Review, and we've talked about UPIC. UPIC also is limited to incoming corporate credits; it cannot be used for corporate debits or consumer-based transactions. If you have an interest in setting up a UPIC, then certainly contact our ACH product group with regard to the process.

Let's talk a little bit about anecdotal issues that have occurred in 2010. We have worked with Fortune 1000 clients that have deployed other mechanisms in which to prevent themselves from being hit by fraud or potential fraud. Some of the things that they've deployed require monitoring. When our client originates an ACH payment file, it's as important — if not more so — to validate that the information that was received at the bank is equal to and exactly the information that was remitted by the originator. Some of the things that our clients have deployed in 2010 include utilizing what we call a mirror file or a companion file to validate veracity of the input data that client has remitted to the bank.

In this scenario the client originates an ACH file to J.P. Morgan, and J.P. Morgan within several hours remits a detail-level granular type of file in the client's required format to validate all of the accounts and all of the payments that have been rendered on behalf of that company. That company in turn validates the input method. It validates the account information and ensures that there's been no change within that information upon receipt by J.P. Morgan on their behalf. If there is an issue, then the client brings it to our attention as quickly as possible. This is a good risk-mitigate with regard to ensuring that the data that was processed is the data that was received. Other types of information can be sent back on a more high-level basis, whether it be from a file, item count and dollar amount, or on a batch level to our client base, but none offers the type of detailed granular type of validation that occurs within the process as does the mirror file.

Let's talk about the process from the originator's standpoint. A lot of our clients ask how they can prevent fraud in terms of monitoring the accounts that are used, for example, for an ACH debit. What we find is an excellent tool is the ability for that corporation to employ something that's known as micro-deposits in order to validate both the identity of and the veracity of the account information that is being used, let's say, for either an insurance premium collection, for a cable bill collection, for a phone bill, or for a credit card bill. When somebody enrolls for an ACH transaction, something known as an authorization is required. However, the use of a micro-deposit, which typically consists of two small-dollar transactions — in other words, a transaction for, let's say, \$.52 and one for \$.85 — is sent to the party that enrolled. When that party receives the \$.52 and \$.85 transaction, usually within one or two business days, they then go online and check their banking information. They notice that they've received a \$.52 and an \$.85 transaction, and they utilize that four-digit code to complete the authorization. The ability for the corporation to know that account is not only up-to-date, but also valid in terms of its identity, is very important in this day and age.

Obviously, this is not always utilizable with regard to a very quick settlement or, let's say, a web or tel transaction that requires a near-instantaneous enrollment, authorization, and settlement. But for a recurring type of payment or if the corporation were to extend the authorization process to incorporate a micro-deposit, it's something that we recommend. The other aspect here is that over time pre-notifications, which is a zero-dollar transaction used to validate the information of the account, is not always utilized by the receiving bank to return back to the originator whether or not the information is valid or not. However, an actual money-bearing transaction always is, so hence, also another reason to utilize what we call a micro-deposit.

Let's talk about other things that can be done with regard to the process, and this is something both the bank, J.P. Morgan, and our client has some responsibility with. One is for monitoring ACH returns. It's extremely important that any type of ACH return be scrutinized for the reason that it was returned for, and that you learn something from it. One of the things that we've deployed at J.P. Morgan is known as preemptive payment intelligence or artificial intelligence to correct information on a transaction and provide that information, if our client wants to receipt it back to our originator. However, if a return does occur, it's important to understand that if it was returned, why it was returned, especially if an item was returned for unauthorized, or the client claims that they revoked the authorization for the transaction. These two types of returns, which are both comprised under Regulation E, indicate that there could be an issue with regard to the business model in place. Either the information was not provided to the customer, or the consumer in this

case, on a timely basis, and they may not be aware of the payment. In other words, it may be an annual or biannual payment, and they may not have received the information that discusses it. Or there's an issue with regard to the actual type of product being sold to the customer, or they have buyer's remorse. Obviously, there are certain types of transactions where maybe it doesn't make sense for an ACH debit to occur, but if pains are taken to ensure that the rationale, the notification and communication with the customer is obtained along with that notification and authorization that's received from the customer, then the program can be quite successful.

Some of the risk-monitoring tools that J.P. Morgan utilizes includes the monitoring of ACH returns for certain reason codes. The NACHA rules specify that for certain types of transactions, including web transactions that we need to monitor the volume and percentage of ACH returns that also may indicate an issue with regard to that originator. We also monitor ACH transactions for kiting or potential kiting. We monitor for recurring returns in the event that the same item was attempted to be returned again. We monitor for the percentage of returns. Obviously, the more successful the program is, the fewer and less percentagewise the returns happen to be, so have you learned something from that return? And probably most vital of all is are there escalation points within your company in the event that transactions exceed those criteria that have been defined. We certainly have those escalation points at the bank, but it must be said that unless you have a responsible party that is performing an escalation point, then it may serve nobody any good if you have those reports and criteria in place.

So let's sum up what the marketplace looks like today and where it's headed. In 2010 corporates are increasingly looking to make their payments electronically and eliminate the checks wherever possible. There are also looking to accelerate the process where they receive payments electronically as opposed to paper. Everybody's looking to save money, but at the same time they're looking to reduce their risk within ACH. ACH payments, as a rule, have the lowest percentage of attempted fraud and attempted loss of any payment method, but there has been an increase overall, with the increase of ACH transactional activity, of attempted fraud. So therefore, it's extremely important that you deploy some of these methods that we've talked about to prevent yourselves from being a victim of these types of potential frauds.

So again, let's review the deployment from the corporate perspective. ACH Debit Blocks we think are a given along with Debit Filters. ACH Positive Pay or Transaction Review we think should be utilized by corporate practitioners if they take an active role in identifying any incoming ACH transactions. A UPIC can be used if that corporate practitioner does not want to provide their sensitive banking information on a broad basis, so they provide this information via a UPIC so that the counterparty never has access to the customer's actual account number. A mirror file, when originating ACH transactions with a reciprocal validation of those payments, ensures that the actual information that's received is what's being processed. The micro-deposits help identify the validity of the account along with the ownership of the account — and extremely important — to prevent any type of loss downstream.

Other types of reports include monitoring for the payment activity that has occurred and ensures that there are parameters put around any returns, and if they exceed a certain boundary, then those are investigated. These are all tools that are germane to the success of an ACH program. Thanks for listening, and have a great day.

J.P. Morgan is pleased to have brought you the proceeding podcast. For more information on J.P. Morgan Treasury services and products visit our website at www.jpmorgan.com/ts.