NICE · ACTIMIZE

Same Day ACH Fraud Concerns Survey: Preparing for New Threats & Challenges

A NICE Actimize White Paper

TABLE OF CONTENTS

Overview

In September 2016, U.S. payments will forever be changed when NACHA ushers in rules for same day processing of Automated Clearing House (ACH) transactions.

Same Day ACH (SDA) will introduce a range of exciting opportunities, allowing Financial Institutions (FIs) to offer new revenue-generating services, such as Same Day Payroll and Same Day Bill Pay. As importantly, SDA will enable FIs to meet consumer demand for speed, gaining a competitive foothold against Fintech, which sells itself on immediacy.

However, these new opportunities also pose new fraud and operational challenges.

Today FIs have 24 to 72 hours to settle ACH transactions, giving them plenty of time to detect and stop fraud. But as of September of 2016, FIs will be required to process received SDA transactions in as short as two time windows daily, making funds available the same day. That will give them hours, or even minutes (depending on when the transaction is initiated), to detect and stop an attack.

Simply put -- FIs will need to be quicker at detecting fraud and deciding how to handle it

Same Day ACH Implementation Timeline

Functionality	Phase 1 Sept. 2016	Phase 2 Sept.2017	Phase 3 March 2018
Transaction Eligibility	Credits Only	Credits and Debits	Credits and Debits
New File Transmission Times	10:30 am ET 3:00 pm ET	10:30 am ET 3:00 pm ET	10:30 am ET 3:00 pm ET
New Settlement Times	1:00 pm ET 5:00 pm ET	1:00 pm ET 5:00 pm ET	1:00 pm ET 5:00 pm ET
ACH Credit Funds Availability	**End of RDFI processing day**	**End of RDFI processing day**	**5:00 pm RDFI local time**

Why a Same Day ACH Fraud Survey?

The move to faster payments in other markets, such as the U.K. in 2008, resulted in an immediate spike in fraud attempts and losses, which were only controlled after FIs changed their fraud and operational strategies to include faster and real-time detection and processes.

The main goal of this survey was to determine whether FIs are preparing for new fraud threats in Same Day ACH. This is especially important considering there is comparatively little fraud associated with traditional ACH, and FIs often rely on manual detection solutions, which may not be appropriate for a faster payments environment.

What we sought to learn with this survey:

Level of perceived SDA fraud threat

State of current ACH fraud coverage

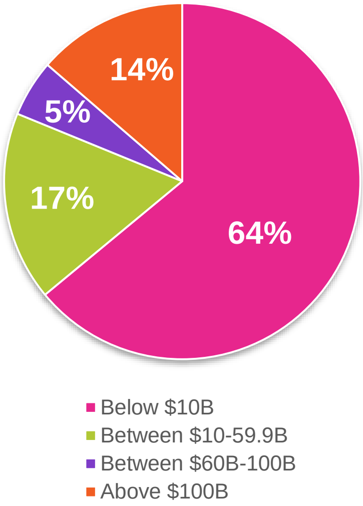
SDA fraud preparedness

Survey Respondents

The Same Day ACH Fraud survey was fielded by a third-party research firm and sent to the NICE Actimize database, as well as through a NACHA newsletter, receiving 60 responses.

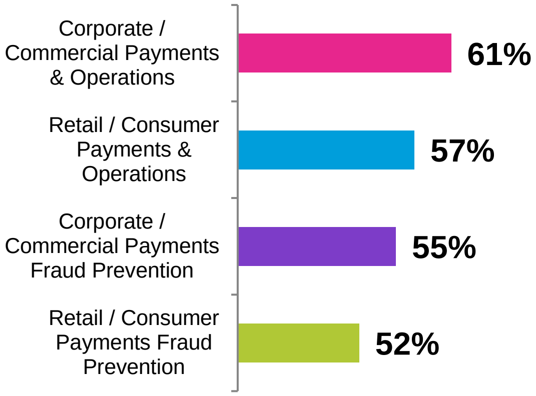
FIs of all sizes (measured by assets) were represented. FIs with assets below $10B dominated the respondent pool, but the overall proportionate breakdown largely matches that of the U.S. FI market.

What we sought to learn with this survey:



Respondents were evenly distributed between corporate and retail environments, and among ACH responsibilities – operations and fraud prevention. Many respondents had overlapping responsibilities in fraud and operations, as well as in retail and commercial banking, which may reflect their roles in smaller institutions where employees wear many hats.

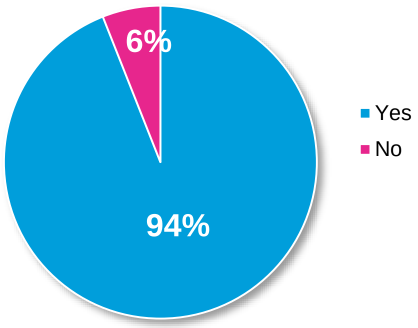
Which of the following ACH functions are you responsible for?



The Big Takeaway: SDA will Result in New Fraud Threats

Survey respondents largely agreed that the move to SDA would pose new fraud threats – and that will require FIs to rethink their current fraud strategies.

Will Same Day ACH pose new fraud threats?



Actimize Insight: FIs Need Fraud Controls in Place before Launching SDA Services
Fraudsters like speed. The faster they can get money out, the better. This is likely the key reason survey respondents almost unanimously agreed that SDA will result in an uptick in fraud threats.

But speed isn't the only factor causing fraud concerns.

Fraudsters routinely target new services and products, where vulnerabilities have not yet surfaced, and have therefore not been covered. The market saw a clear example of this when Apple Pay was first released in 2014, and banks lost tens of millions of dollars to fraud in the first 90 days after launch due to holes in the card provisioning process.

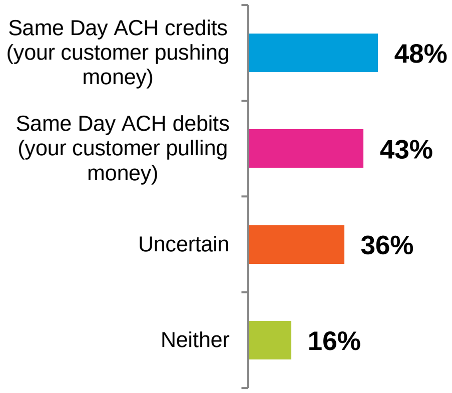
Fraudsters will keep a sharp focus on new SDA services, as well as other emerging faster payments offerings, to discover and exploit the weak spots. Early anecdotal reports show that fraudsters are already beginning to game the traditional ACH system in order to learn how it works in time for the move to SDA.

To prepare for this, FIs must have appropriate tools and policy in place before SDA services go live. It's simpler to tweak policy to stay ahead of emerging threats than it is to begin implementing a new fraud strategy after attacks have started to occur.

FIs Won’t Flock to SDA … Yet

About half of survey respondents said they will originate SDA transactions – though that number is likely to increase.

Which of the following SDA transactions will you originate?

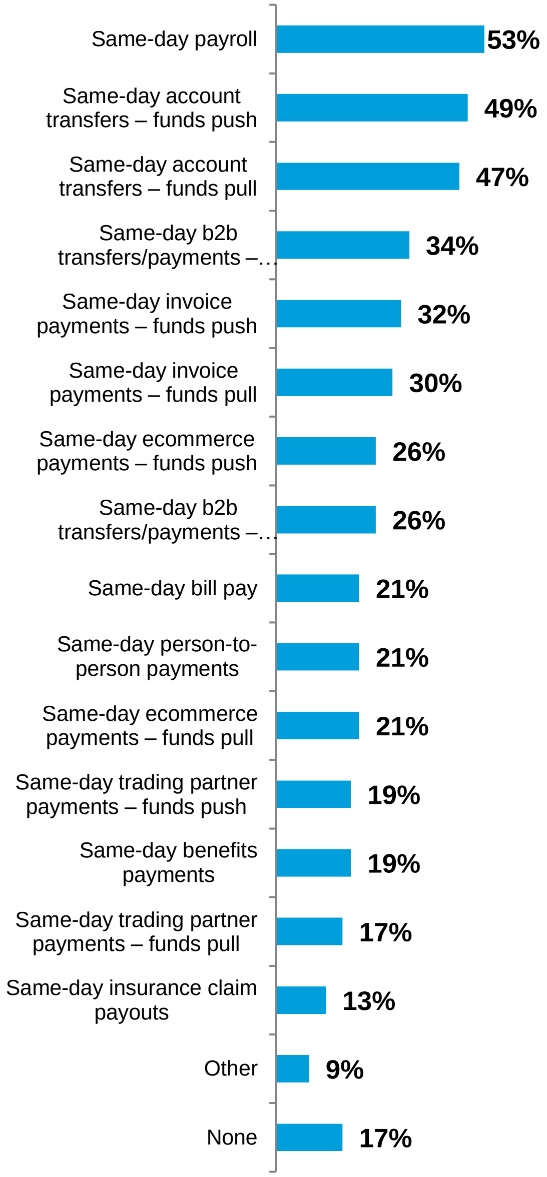


Actimize Insight: The Move to SDA May be Inevitable

More than half of respondents either won’t offer SDA services or are still unsure what they will do. However, we expect these numbers to turn around for a few reasons:

- FIs that don’t offer SDA services will face competitive pressure from those that do
- FIs will need to invest in operational changes to fulfill the requirement to receive SDA transactions, including increased staff and fraud tools. FIs will eventually leverage these investments to support new originating services
- A range of new faster payment types will emerge in the coming years, and FIs will be forced to accommodate them. Some of the SDA fraud strategy investments can be leveraged across faster payments

Which of the following Same Day ACH services will your organization offer?



The State of ACH Fraud Coverage

Many FIs aren’t confident that their existing fraud tools sufficiently cover ACH, according to the survey.

Originated credits are thought to be the best protected ACH segment, with 59% of all respondents (and 83% of respondents in the $10B+ category) saying they have sufficient coverage.

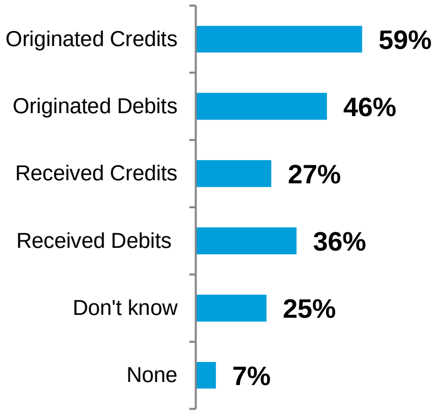
Payments Cheat Sheet

- Originated Credits (your customer pushing money)
- Originated Debits (your customer pulling money)
- Received Credits (someone taking money from your customer)
- Received Debits (someone giving money to your customer)

While a higher percentage of respondents say they have fraud coverage for originated credits, 40% reporting lack of coverage is staggering. Additionally, it is troubling that the smallest institutions report a lower rate of coverage. Fraudsters learn quickly which organizations have sufficient controls and target them first.

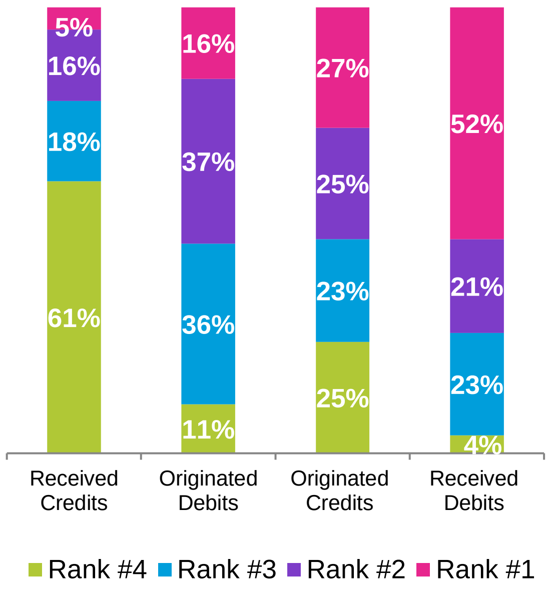
Most notably, though, confidence in coverage drops significantly when it comes to received ACH credits and debits.

For which segments of ACH are your current fraud controls providing sufficient fraud prevention and detection?



Originated and Received Debits - a Focus of Concern

Which of the following Same Day ACH services will your organization offer?



Actimize Insight: Fraud Concerns driven by more than Liability

The highest majority of respondents had concerns about fraud in received debits, with 73% placing it as their first or second greatest concern. Meanwhile 53% pointed to originated debits as their first or second greatest concern.

Why the intense focus on debits? There are a couple of explanations here:

1. While many FIs have focused on fraud coverage for originated credits, FIs may now be bracing for new NACHA rules, which require them to begin receiving SDA credits in September 2016, and then SDA debits a year later in September 2017.
2. But concerns go deeper than looming deadlines, and they differ for originated and received debits. With originated debits – where money is leaving the institution – liability concerns abound. However, for received debits – where customers are on the receiving end of a transaction – FIs are concerned that detected fraud will worry customers enough to shut down their accounts, either to start a new one, or even to leave the institution. Both scenarios result in significant financial burden to FIs.
3. FIs are also seeking more complete fraud coverage for faster payments, with a holistic view of money-in and money-out across channels. After all, monitoring and scoring unusual movement from an account (a received debit), stops the money from leaving the account with the fraudster. We also expect FIs to request the ability to analyze the correlation of money-in and money-out across channels to stop faster payments fraud.

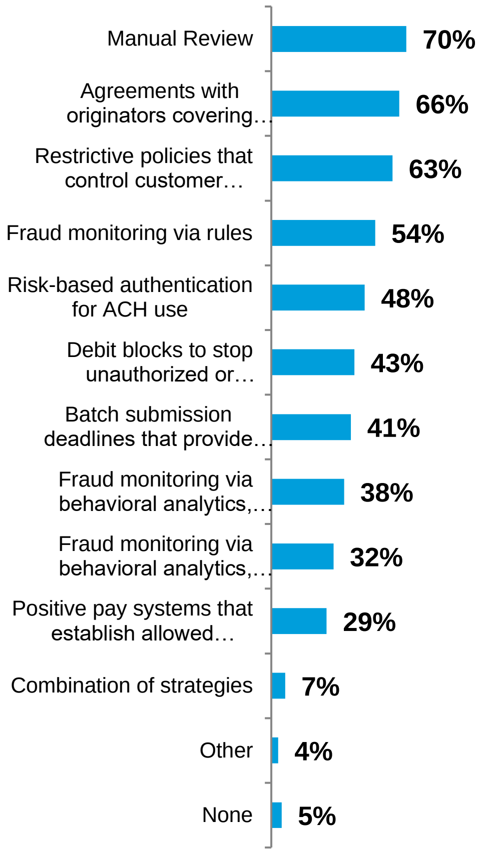
How Will FIs Change their Fraud Strategies?

In short, the days of manual review processes and weak authentication for ACH are over.

It's not that FIs will eliminate their existing fraud tools (which are often manual), but they'll look for detection methods that keep up with faster transactions.

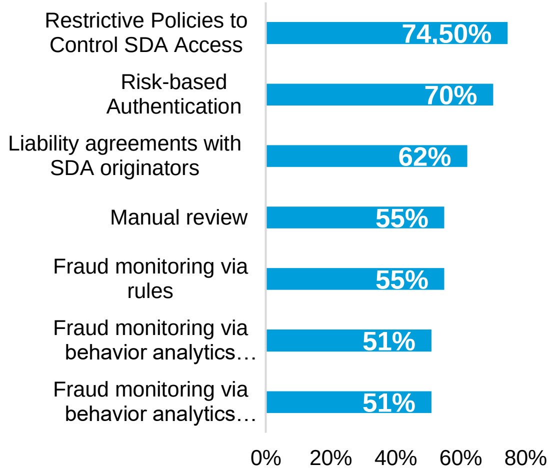
When asked what kind of fraud controls are place for ACH today, nearly 70% pointed to manual review for resolution – but that number drops dramatically when respondents are asked what kinds of fraud tools they'll need for SDA.

What kind of fraud controls do you have in place for ACH today (before Same Day ACH)?



Things change dramatically when respondents are asked what fraud tools and tactics they'll need to prepare for SDA.

What fraud tools and tactics will you need for SDA?



Actimize Insight: FIs Are Look to Authentication and Away From Manual Review

Catching fraudsters before they get into the system:

The need for risk-based authentication jumps to 70% for SDA from 48% for traditional ACH. The shift signals a need to keep fraudsters out of the system in order to protect faster payments. Investing in risk-based authentication will allow FIs to make real time decisions on user access at log in (at authentication) and before every faster payments transaction throughout a session.

Creating Restrictive Access Policies:

Use of "restrictive policies to control ACH access" jumps to 74.5% for SDA from 63% for traditional ACH -- another indication that FIs will take steps to keep fraudsters out of the system. It's likely that FIs will write access policy that provides SDA services only to lower-risk customers, gradually loosening reigns as they learn to secure a new faster environment.

Eliminating manual review:

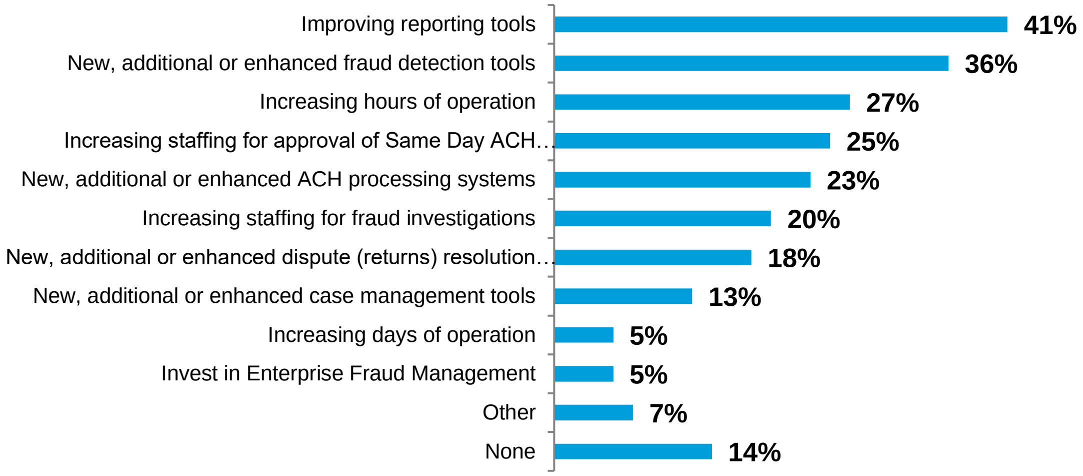
The anticipated use of manual review for ACH fraud detection drops significantly from 70% to 55%. This isn't surprising since manual review can be slow and won't fit the bill for the short windows of time in which SDA transactions will be processed.

The rise of behavior analytics for ACH fraud detection:

Use of fraud monitoring via behavior analytics is likely to rise for SDA, with 51% of respondents saying they'll use this strategy for fraud detection in the channel and the back-end for SDA as compared to 38% and 39% respectively for traditional ACH. We expect this number to grow further. In markets that have moved to faster payments across the world, anomaly detection using advanced analytics has been central to controlling fraud in real time.

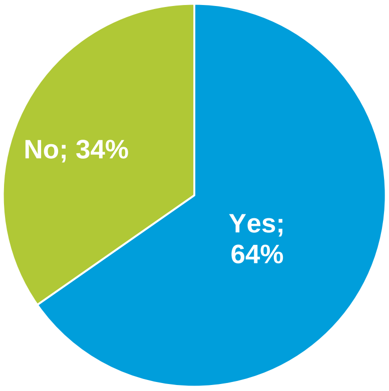
FIs will need to make operational changes to prepare for SDA

Which of the following operational changes will you institute to prepare for Same Day ACH?

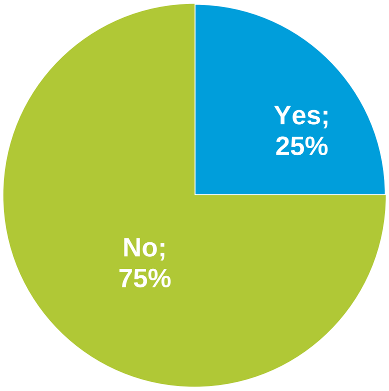


FIs foresee allocating additional budget for fraud and operational changes to prepare for SDA

Do you anticipate the need for additional budget to pay for improvement in fraud controls for Same Day ACH?



Do you anticipate additional budget to pay for ACH system or operational changes to support Same Day ACH?



Actimize Takeaways: Steps to Prepare for Faster and Instant Payments

Key elements to supporting a faster payments environment

Intelligent Authentication

Analytics & Fraud Risk Scoring

Fraud Strategy & Decisions

Operations & Case Management

The movement to Same Day ACH is a first major step toward faster payments in the U.S.

In the coming months and years, FIs will begin offering instant P2P, bill pay and account transfers. At first these will be optional services, but eventually immediate payments will be ubiquitous.

The good news is that investments in fraud strategy and operational changes to support SDA services can be leveraged for the faster payments long haul.

In preparing for SDA and other faster payments, Actimize suggests a multi-layered strategy, which combines authentication management, behavior analytics and a specialized operations strategy to support and prioritize faster payment transactions and services.

Intelligent Authentication Management

Many FIs will implement risk-based authentication as one way of coping with fraud concerns in an SDA environment. This approach should be bolstered with intelligent authentication management, which should include the following capabilities:

- Risk-based decisions at log-in and throughout a session for each interaction
- Management of many authentication methods across channels, making real-time step-up decisions among these tools based upon the risk of an event, cost efficiency and customer preference, among other factors
- Ability to write authentication strategy rules that are specific to faster payments; for example, leveraging more stringent authentication challenges for high-amount, fast transactions. Users must also have the agility to modify these rules as new threats emerge.

Analytics and Real-Time Fraud Risk Scoring

As FIs transition to instant payments, they'll need fraud analytics tools that identify risk and make decisions as fast as the money moves.

These tools build customer-level profiles to establish a baseline of normal or typical behavior and then spot anomalies indicative of fraud. Anomalies might include a combination of new payees, in suspicious regions, stemming from an unusual user device, for example. These fraud detection tools also monitor channel data and have a deep understanding of monetary and non-monetary events, such as changes on the account servicing.

The desired output of these analytics is a fraud risk score that combines all the vectors of the customer activities relating the transaction: the event, the channel, the device, and behavioral history between the counterparties.

Fraud Strategy Rules for Faster Payments

Generating fraud risk scores is an important first step, but this must be supported by strategy rules that are designed specifically for a faster payments environment.

Fraud strategists should be able to write simple business rules, so that risky payments and events can be automatically declined, delayed or further authenticated in real time.

It's important for an organization to write rules that reflect its risk appetite on faster payments, weighing security and customer experience.

Operations and Case Management for Faster Payments

Lastly, a fraud management system needs to have a central alert and case management system which enables the prioritization of SDA or other faster payments alerts. This gives FIs the ability to create cases and start investigations in a separate workflow.

This approach should include dynamic SDA reporting from investigations, which must be linked to appropriate customer outreach.

All-in-all, as payment methods speed-up, it is critical to streamline fraud management processes so that fraud risk analysis can occur immediately, and decisions can be automated, reserving the human-element for the most risky manual review of prioritized alerts in real-time.

Special Considerations for a Commercial SDA Fraud Plan

It's important to note the separate considerations must be made to prepare for SDA in a corporate banking environment.

Fraud detection tools for SDA in a commercial environment must include the following capabilities:

- Analyze overall batch
- Analyze individual entries
- Create company and individual profiles, considering suspicious activity linked to an organization and all of the individuals that act on its behalf
- Investigation tools for batch and single entry
- Aggressively windows on batch analysis and detection

Conclusion

Concern in the transition to SDA or any other faster payments system is to be expected – but these changes are inevitable.

The best way to prepare for the potential uptick in fraud threats linked to faster payments is to have a strategy in place before you implement new services. It will be much simpler to tweak and alter fraud controls according to need than it will be to begin implementing systems after attacks are in full force.

Now is the time to assess your current fraud controls and strategies, and then begin to build a plan.

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.

info@niceactimize.com | www.niceactimize.com | www.niceactimize.com/blog | @nice_actimize | linkedin.com/company/actimize

NICE · ACTIMIZE