Fraud Trends & Prevention Insights

APT US&C 2019 Annual Conference | July 2019

Brian S. Anderson, Executive Director
Commercial Banking

J.P.Morgan

Chase, J.P. Morgan, and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, “We”, “Our” or “Us”, as the context may require).

We prepared this document and associated presentation materials for your sole and exclusive benefit. These materials must be used for discussion purposes only, and are incomplete without a related briefing provided by our representatives. While we are providing the materials and briefing, we are not making a commitment to provide any product or service at this point. This information is confidential and proprietary to our firm and may only be used by you to evaluate the products and services described here. You may not copy, publish, disclose or use this information, in whole or in part, for any other purpose unless you receive our express authorization.

In preparing the information, we have relied upon, without independently verifying, the accuracy and completeness of publicly available information or information that you have provided to us. Our opinions, analyses and estimates included here reflect prevailing conditions and our views as of this date. These factors could change, and you should consider this information to be indicative, preliminary and for illustrative purposes only.

The information is not intended and shall not be deemed to contain advice on legal, tax, investment, accounting, regulatory, technology or other matters. You should always consult your own financial, legal, tax, accounting, compliance, treasury, technology, information system or similar advisors before entering into any agreement for our products or services.

This Information is provided as general market and/or economic commentary. The information is not J.P. Morgan research and should not be treated as such. In addition, the information does not constitute advice or a recommendation regarding the issuance of municipal securities or the use of any municipal financial products or, the advisability of acquiring, holding disposing of, exchanging or otherwise taking action regarding, or as to the management of, securities or other investment property. We are not providing any such advice. We are not acting as your agent, fiduciary or advisor, including, without limitation, as a Municipal Advisor under Section 15B of the Securities and Exchange Act of 1934, as amended or under, or with respect to assets subject to, the Employee Retirement Income Security Act of 1974, as amended.

The information does not include all applicable terms or issues and is not intended as an offer or solicitation for the purchase or sale of any product or service. Our products and services are subject to applicable laws and regulations, as well as our service terms and policies. Not all products and services are available in all geographic areas or to all customers. In addition, eligibility for particular products and services is subject to satisfaction of applicable legal, tax, risk, credit and other due diligence, JPMC’s “know your customer,” anti-money laundering, anti-terrorism and other policies and procedures.

Products and services may be provided by Commercial Banking affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those that can be provided by Commercial Banking affiliates will be provided by appropriate registered broker/dealer affiliates, including J.P. Morgan Securities LLC and J.P. Morgan Institutional Investments Inc. Any securities provided or otherwise administered by such brokerage services are not deposits or other obligations of, and are not guaranteed by, any Commercial Banking affiliate and are not insured by the Federal Deposit Insurance Corporation.

All trademarks, trade names and service marks appearing in the information are the property of their respective registered owners.

J.P.Morgan

2018 Payments Fraud Themes

New record level of payments fraud

ACH sees increase in fraud

BEC* and sophisticated fraud

Larger organizations bigger targets for BEC

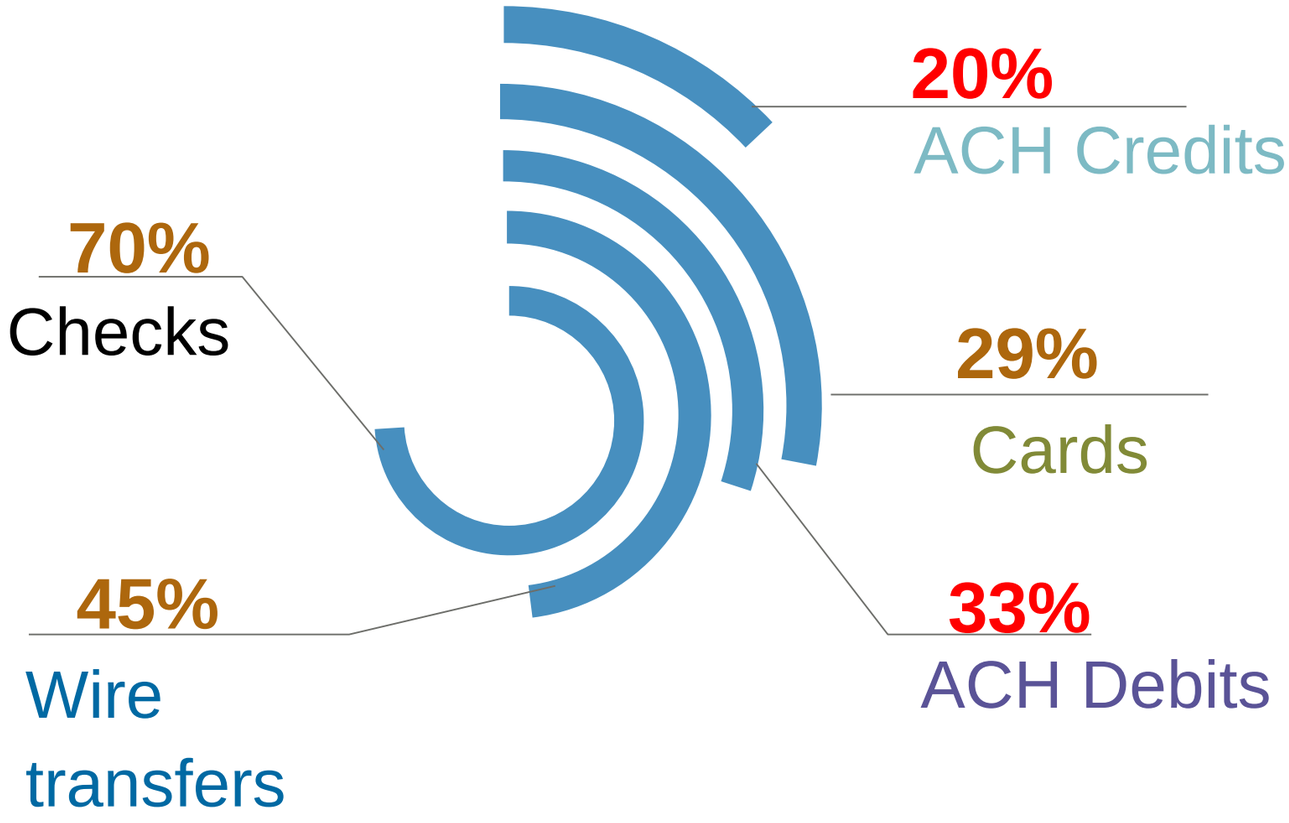
ACH sees big increase as target for BEC

Phishing may be more of a problem than you think – Be Aware

Source: 2019 AFP Payments Fraud and Control Survey
*BEC: Business Email Compromise

Know your risk – fraud by payment method

Targeted payment method for fraud (% of organizations)[1]



Checks

- Payment method most subject to fraud

Wires

- BEC most likely the cause

Cards

- Continues to decline

ACH Debits

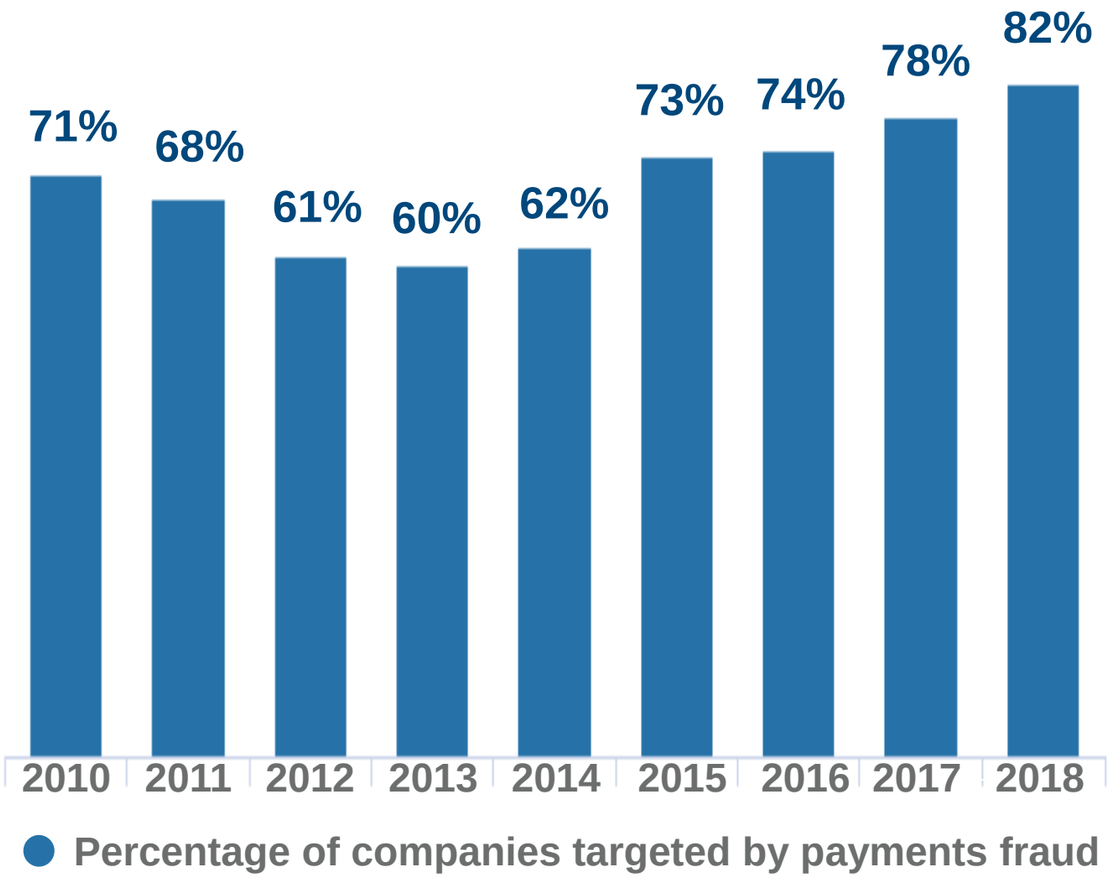
- Increased to record level

ACH Credits

- Dramatic increase compared to previous trend

[1] Source: 2019 AFP Payments Fraud and Control Survey

Payments Fraud Activity Surged in 2018



Experienced Payments Fraud Attacks in 2018

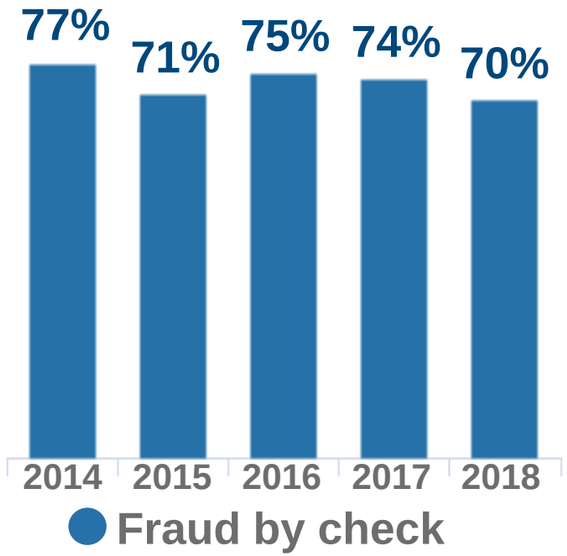
69%

Of businesses with annual revenue less than $1 billion

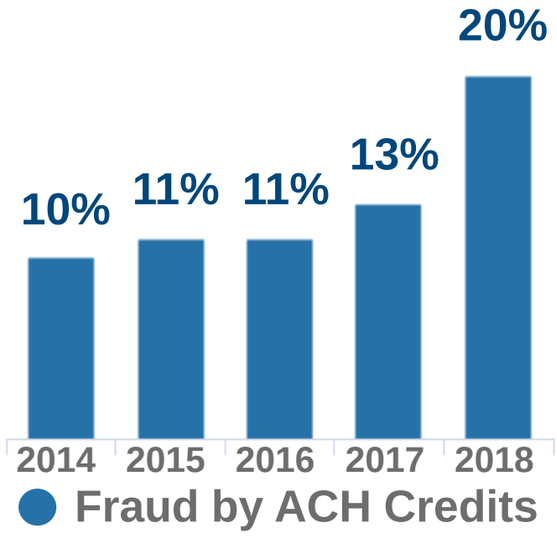
87%

Of business with annual revenue at least $1 billion

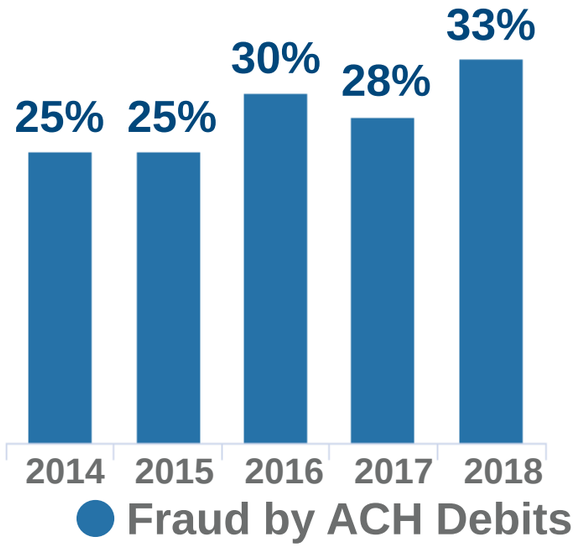
Check Fraud Drops Slightly but ACH Fraud Increases



Check



ACH Credits



ACH Debits

Not all fraud is unauthorized: < ½% of fraud is unauthorized[1]

Unauthorized Fraud

Challenges:

- Fraudster sends/pulls money out of victim's account
- Malware
- Data theft
- Social engineering

Recommendations:

- Monitor account activity
- Leverage channel access, device and location information
- Monitor for bots
- Use fraud solutions

[1] NICE Actimize & NACHA Faster Payments Fraud Management Webinar 2019

Not all fraud is unauthorized:< ½% of fraud is unauthorized[1]

Authorized Fraud

Challenges:

- Customer tricked into sending funds to someone other than intended recipient for a purpose they believe to be legitimate
- Social engineering

Recommendations:

- Educate, Educate, Educate
- Leverage strong payment and amount analytics
- Validate, validate, validate
- Think holistically
- Take a risk based approach

J.P.Morgan

[1] NICE Actimize & NACHA Faster Payments Fraud Management Webinar 2019

Email Scams Grow More Sophisticated

Survey respondents reported the following common BEC attacks:

81%

Spoofed email addresses

44%

Impersonate vendors in emails

33%

Pretend third parties in emails

- Business email compromise (BEC) targets businesses and individuals responsible for initiating payments.
- Eighty percent of organizations were exposed to BEC scams in 2018—the highest number on record.

How Organizations Are Defending Themselves

Ways financial professionals are protecting their companies include:

88%

Use Positive Pay to verify the authenticity of checks

68%

Perform daily reconciliation of check activity

72%

Segregate accounts

65%

Perform daily reconciliation of ACH debits

How organizations are protecting themselves (continued)

Check

- Positive Pay
- Payee Verification
- Reverse Positive Pay
- Reconciliation
- Post No Checks
- Check Encashment
- Check Print
- Stop Payments

ACH

- Transaction Review
- Debit Blocking
- UPIC
- VRN
- Account Owner Authentication

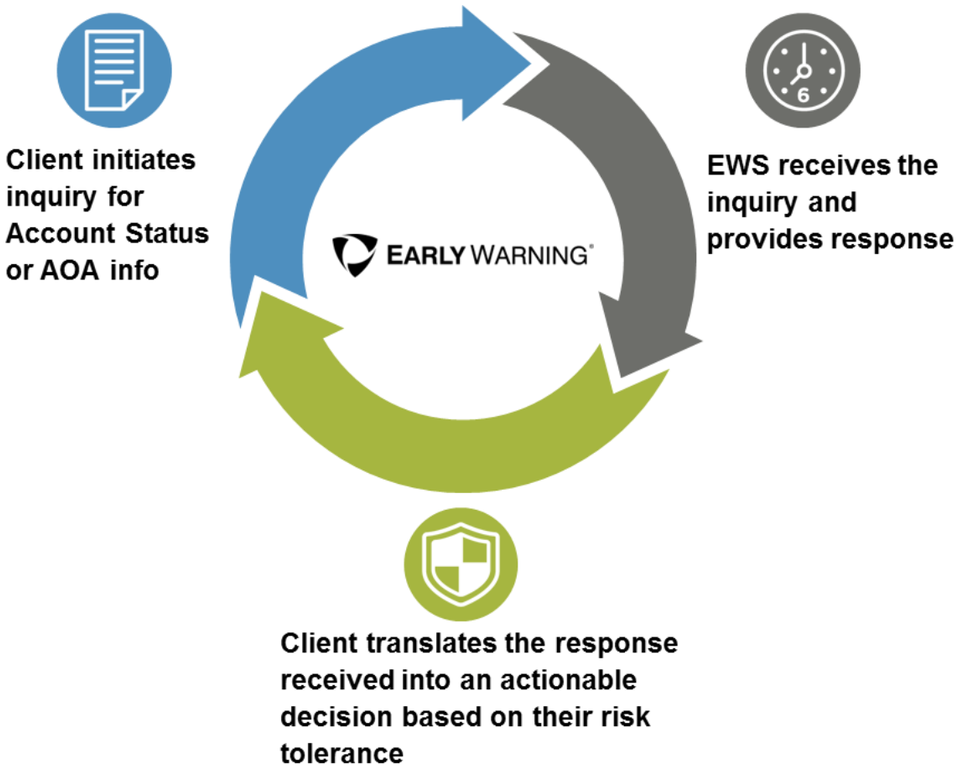
How organizations are protecting themselves

Business Email Compromise (BEC)

- No Payment Initiation from Email
- End-user BEC Education
- Verification Changes
- Two-Factor Authentication
- Phone Confirm Transfers
- Intrusion Detecting
- Color-coded Email
- Flag Email with Different Reply Address
- Penalties for Opening Phishing Emails

Fraud Protection Services: Account Owner Authentication

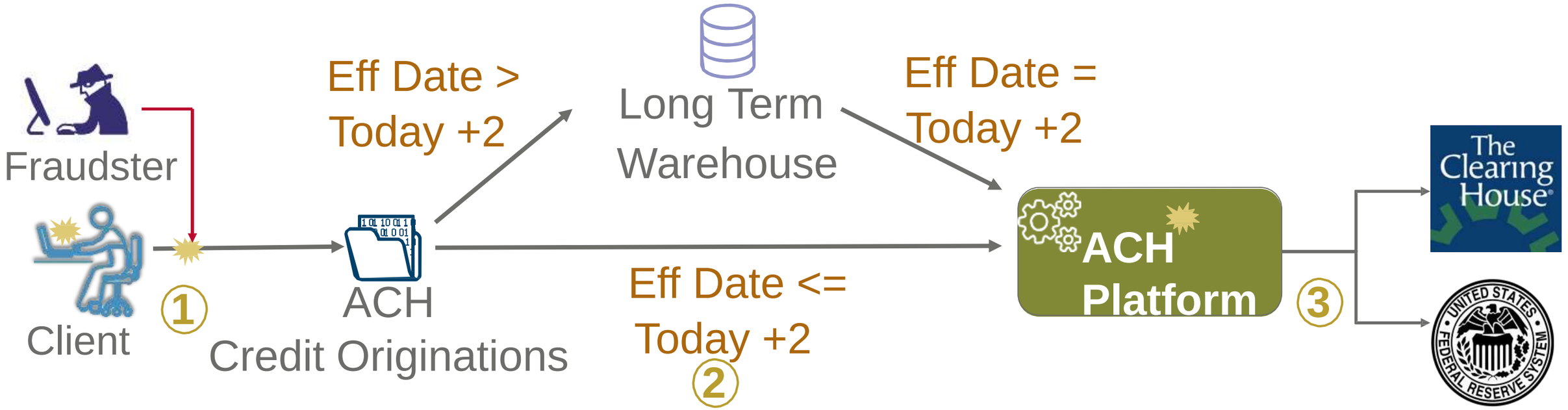
Early Warning Services



Provides answers real-time :

- Does the account exist (open/active)?
- What is the account's associated risk?
- Is the person authorized to transact on this account?
- What is the likelihood of the item being returned?
- Is the account a non-DDA Account?

ACH Fraud Monitoring - Traditional



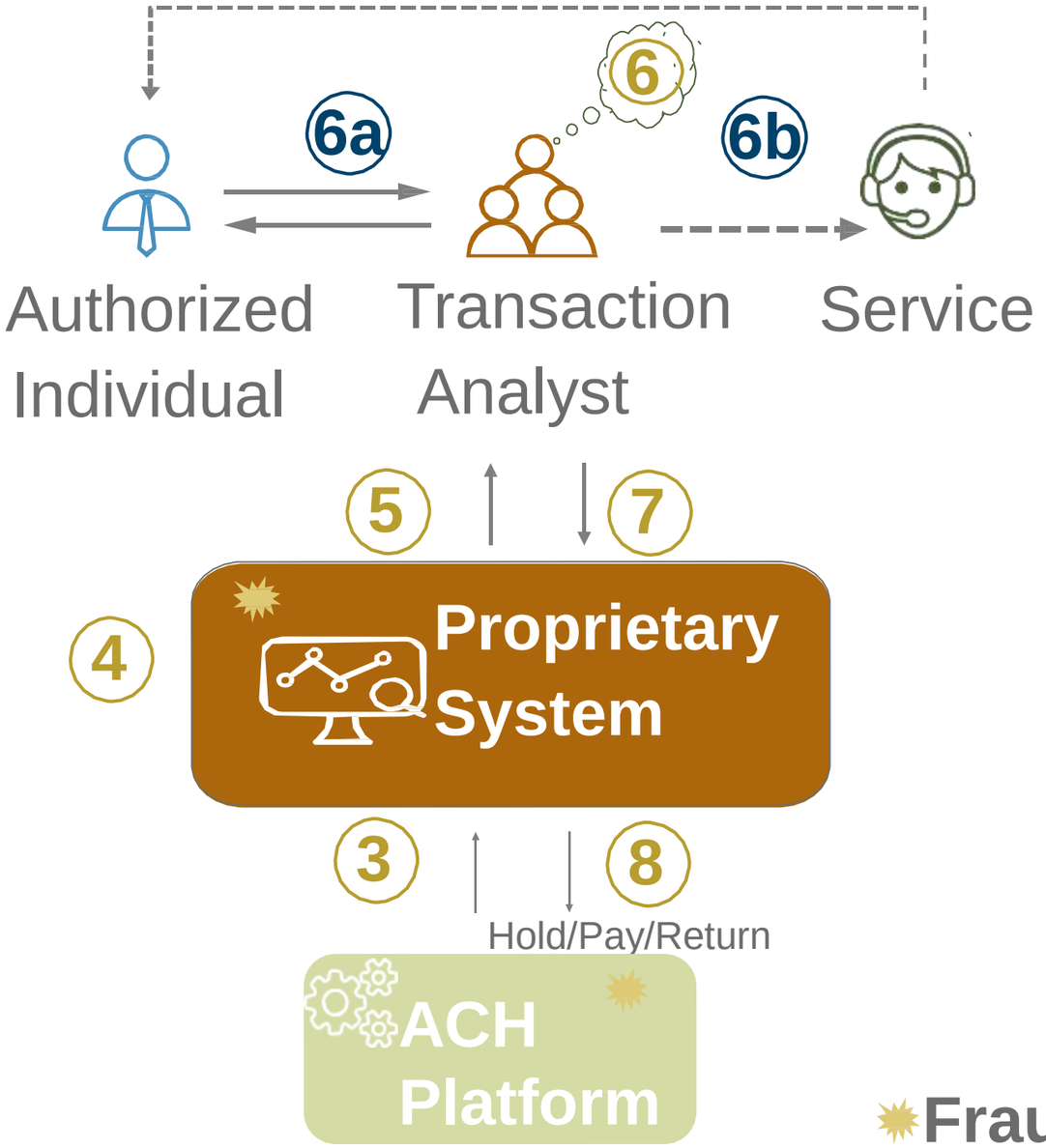
Steps

1. ACH Transaction/Batch Initiated
2. ACH sent to ACH Platform
3. Transactions sent for Processing

Fraud Mitigation Efforts

J.P.Morgan

ACH Fraud Monitoring – Looking for unusual activity



3. ACH credit transactions are sent to proprietary System
4. System performs analytics on ACH credits
5. Sends unusual ACH credits to Analyst queue
6. Analyst reviews ACH credit transaction to decide:
   - 6a Review transaction(s) with Client
   - 6b Service engages Client to contact Analyst
7. Analyst sends decision to System
8. ACH Transactions are sent for processing

J.P.Morgan

Fraud Mitigation Efforts

Questions