PAYMENTS NEWS FOR BUSINESS CUSTOMERS

1st Quarter 2020

ACH Network Continues to See Growth

The ACH Network saw a remarkable year in 2019 as the annual growth rate reached a 12-year high. Below are some highlights:

- There were 24.7 billion payments on the ACH Network, an increase of 7.7% over 2018. The value of those payments was $55.8 trillion, up nearly 9% from 2018.
- It was the seventh consecutive year in which ACH Network value increased by more than $1 trillion, and the fifth straight year to notch a volume gain of more than 1 billion payments.
- Business-to-business (B2B) payments continued to be a solid growth area for the ACH Network, increasing 12% last year to 4 billion payments. Direct Deposit of payroll and other payments to consumers was up 6% to 7.2 billion payments, while internet payments rose more than 13% to 6.7 billion.
- Same Day ACH continued its impressive rise, finishing the year with a record 250.4 million Same Day ACH payments with a total value of $247 billion. Those are increases of 41% and 55% respectively.

FBI: Business Email Compromise Cost Businesses $1.7B in 2019:

BEC attacks comprised nearly half of cybercrime losses last year, which totaled $3.5 billion overall as Internet-enabled crimes ramped up.

Business email compromise (BEC) attacks cost organizations an estimated $1.77 billion in losses in 2019, reports the FBI, which received a total of 23,775 complaints related to this threat.

The FBI's Internet Crime Complaint Center (IC3) this week released its "2019 Internet Crime Report," which digs into cybercrime trends throughout the year. In 2019 the IC3 received 467,361 complaints, which cost organizations $3.5 billion overall – up from $2.7 billion in 2018.

The most frequently reported complaints relate to phishing and similar attacks, non-payment/non-delivery scams, and extortion, officials say. But the most expensive complaints are related to BEC, romance or confidence fraud, or copying the account of a person or vendor to collect personal or financial data about a victim familiar with them, according to the report.

BEC attacks, also known as email account compromise (EAC), are constantly evolving as adversaries become more sophisticated. Back in 2013, scams often started with the spoofing of a CEO's or CFO's email account. Fraudsters sent emails appearing to come from these execs to convince employees to send wire transfers to fake accounts.

Since then, BEC has evolved to include the compromise of personal and vendor emails, spoofed lawyer email accounts, and requests for W-2 data. Attackers often target the real-estate sector and/or make requests for

expensive gift cards. In 2019 IC3 saw an increase in BEC complaints related to the diversion of payroll sums: Attackers send a fake email to a human resources or payroll department requesting an update to a specific employee's direct deposit information.

"The attackers are looking for new sources of revenue from people," says Erich Kron, security awareness analyst at KnowBe4. "For example, instead of just going after wire transfers, something that people are becoming aware of, they have changed to redirecting paychecks to different accounts or getting people to purchase a large number of gift cards, then having them send the card numbers and information under the guise of an executive rewarding employees or thanking vendors."

Kron also points to a rise in hybrid attacks in which a victim receives an email making a request and simultaneously receives a text message from a spoofed number designed to seem like the same person, saying they sent an email. It's a highly targeted but effective technique, he says, and it's less commonly known than wire transfers. Victims trust the second request source. Phishing and BEC attacks impersonating specific people reached 32% between October and December 2019.

Upcoming NACHA Rule Alert: New Return Code R11 Becomes Effective April 1, 2020

The National ACH Association has approved a rule change regarding clarification of unauthorized return types to more clearly instruct the ACH Originator of the reason for the reject at the Receiver's institution. It is important in preparation for this new rule that you train your staff on (1) understanding the meaning of this return reason code and (2) understanding appropriate actions to take when receiving this return code from our financial institution.

WHAT DOES THIS RULE DO?

The rule re-purposes an existing, little-used return reason code (R11) that will be used when a receiving customer claims that there was an error with an otherwise authorized payment. Currently, return reason code R10 – *Customer Advisors Unauthorized Improper, Ineligible, or Part of an Incomplete Transaction* is used a catch-all for various types of underlying unauthorized return reasons, including some for which a valid authorization exists, such as a debit on the wrong date or for the wrong amount. In these types of cases, a return of the debit still should be made, but the Originator and its customer (the Receiver) might both benefit from a correction of the error rather than the termination of the origination authorization. The use of a specific return reason code (R11) enables a return that conveys this new meaning of "error" rather than "no authorization." This differentiation will give ODFIs and their Originators clearer and better information when a customer claims that an error occurred with an authorized payment, as opposed to when a customer claims there was no authorization for a payment. ACH Originators will be able to react differently to claims of errors, and potentially could avoid taking more significant action with respect to such claims.

Return Reason Code R10 will be defined as "Customer Advises Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receiver's Account".

Return Reason Code R11 will be defined as *"Customer Advises Entry Not in Accordance with the Terms of the Authorization."* It will be used by the RDFI to return an entry for which the Originator and Receiver have a relationship, and an authorization to debit exists, but there is an error or defect in the payment such that the entry does not conform to the terms of the authorization.

CONTACT US WITH QUESTIONS: Let us know if you have any questions. We are happy to provide you with additional information on how to protect your account and comply with network rules and regulations.