EARLY WARNING®
Collaborative intelligence. Trusted exchange.

Consideration Brief

Vulnerabilities and Risks Must Be Considered as Industry Ponders New, Faster Payment Systems

By Laura Weinflash, Vice President, Product Management at Early Warning Services

The financial services industry has witnessed ongoing innovation around faster payments, including real-time payment notification and may include near real-time settlement. The Federal Reserve has taken the lead in providing thought leadership around faster payments. NACHA is moving toward same day settlement of ACH and various organizations in the market are considering or developing innovative payment schemes to enable faster information about payments as well as consideration for real time settlement.

Early Warning has been a leader in fraud prevention and risk management for more than two decades. We see value in the industry dialogue around the proposed development of a faster payment system in the U.S.; however, Early Warning and our participant banks and credit unions share concerns with others in the industry that a near-time or real-time enhanced payment system may also inadvertently introduce new vulnerabilities that fraudsters and criminal may exploit.

We have seen similar vulnerabilities emerge in the U.K. when faster payment systems were introduced. In recent years there has been a proliferation of fraud in the U.S. The latest numbers from the American Bankers Association support this: ACH fraud is trending upwards, as is card fraud, check fraud and account takeover fraud[1]. In order to help prevent the growth of fraud, we believe there are things that must be considered before enhancing an existing payment system or launching any new proposed payment system. One of the key considerations is collaboration. Collaboration is a foundational piece of Early Warning's business model. Our organization collaborates with other organizations in the financial services industry to help create a safe and secure transactional network and a faster payment system. The following recommendations reflect not only Early Warning's position, but the opinions of many in the industry as well as payment experts seeking to have input in the creation of a new payment system/network to ensure safer, faster payments.

TYPES OF FRAUD, RISK AND COMPLIANCE TO ANTICIPATE WITH FASTER PAYMENTS

In today's U.S. payment environment, we are seeing organized attacks against businesses, consumers and banks routinely occur.   Criminal exploitation of account information in order to commit unauthorized transactions is expected to increase and continue. If money movement becomes near real time using check, ACH or a new system, expect data breaches and account takeover attempts to increase without appropriate risk management protection.

Based on observations from other countries launching faster payments and experiences in the payments business, we make the following suggestions with regards to specific threats and vulnerabilities expected with a faster payment system:

1. **Account Takeover/Third Party Fraud - Authentication**

   a. Plans must be made to ensure tokens are not compromised or vulnerable to malware, phishing schemes and other events where legitimate accounts or tokens are compromised. The consumer and business impact of fraud may be facilitated by faster payments when the financial institution (FI) did not have time to bring a suspect transaction to the attention of the client before the funds were gone. This could negatively impact consumers and businesses that fall victim to account takeover or other fraud schemes. If adequate steps are not taken, expect an increase in consumer and business victims.

[1] Deposit Account Fraud Survey Report, the American Bankers Association, December 2013.

Any proposed new payment system will need to provide insight to the FI approving the transaction and give enough time to validate the legitimacy of the transaction. This may take time to validate with the account holder. An immediate settlement system needs to have time allocated for investigation and confirmation either before the funds are sent, or the ability for the receiving bank to hold the funds for a period of time in order for the paying bank to confirm the transaction is authorized by the legitimate accountholder.

Information in a real-time payment system includes validating the type of authentication done; knowing more details about the transaction is a must. FIs need the ability to block tokens/accounts that are suspected or actually taken over. With any new system, it will be important to determine how the bank and payment acceptor will know if and when the credentials have been re-instated. There needs to be a method to know that the token is being used by a legitimate customer or a fraudster.

b. Recommended approaches to detecting account takeover include:

i. Score in *real time* the transaction of the sender and intended receiver to know the likelihood that the transaction is valid. This also includes seeing in real time every event including each transaction.

ii. Ensure there is a way to know that the transaction originator has completed the minimum standards required to authenticate that the person initiating the transaction is an actual account holder. (Consideration should be given to including an indication of the type of authentication used.)

iii. Ensure a FI has methods available to stop a transaction if it fails authentication, or if it appears that the account has been taken over.

iv. Include a function that enables a recall of a transaction should the customer change their mind or account takeover is suspected.

2. First Party Fraud

a. First Party Fraud, where an actual account holder (or fraudster using a created, synthetic identity) finds ways to "game" the system. First party fraud is a growing problem and any proposed faster payment system will need to ensure it includes methods to detect and prevent first party fraud.

Also, false fraud claims can be expected. "I never made that purchase" "I never received the goods" are common examples. A new system will require the ability for the bank and the originator to detect if the person's claims are false. The system should include specific data to determine if such claims are true.

3. Non-Sufficient Funds Risk/Customer Service Issues

Expect consumers and businesses to be negatively impacted if unauthorized access or posting orders of other access methods to the account occur.

a. If the check, debit, ACH and or wire settlement times become more immediate, there will be additional risk associated with these transactions. The posting order of items will need to be re-addressed, analyzed and changing customer expectations will need to be considered.

b. In the event a new faster payment system is built and linked to the traditional checking account, additional NSF/Posting risks will occur and risk associated with other instruments such as check, ACH, debit and wire could increase.

c. This system may also need to take into account overdraft limits and shadow limits and lines of credit tied to the deposit account.

4. OFAC/BSA/KYC/Compliance

a. The faster payment system should include additional time to screen to ensure the senders and recipients are legally able to send and receive funds. This includes Know Your Customer (KYC), Office of Foreign Asset Control (OFAC) screening, and Bank Secrecy Act (BSA) compliance requirements. Mechanisms must be in place to ensure that transactions associated with people or businesses that are included on government watch lists be flagged, stopped and investigated, before funds are delivered and or released in which the OFAC response could be more than 24 hours.

b. In a near real-time or real-time system, fraudulent transactions could result in funds quickly moving from account to account and then out of the country. With this in mind, there is a need to track the velocity and movement between accounts in order to detect money laundering or account takeover and retrieve the funds.

5. Operational Risks

- **a.** There are multiple operational risks that may come with faster payments and faster settlements. Requirements include ensuring the system has the ability to validate an account number is accurate, it belongs to the person initiating the transaction and that person is authorized to make the transaction. Incorrect account numbers being used is not uncommon, so the system needs the ability to ensure the correct account number is in place while offering the ability to reverse transactions errors occur.
- **b.** Accounts that close may re-open within the day or days following. Consumers and businesses may close an account and then change their mind and re-open the account. The system must be agile and enable the ability to post or reverse transactions in such scenarios.
- **c.** Transparency of information is needed to make faster payment, posting and settlement decisions. As described in the scenario of unauthorized access, there needs to be the ability to block a transaction, block an originator, amount, location, or token should the account be compromised, but keep the actual account open.
- **d.** The system needs the ability to turn off an account system-wide immediately, should be there unauthorized access or other types of fraud.
- **e.** Another important consideration: although most FIs use real-time or near real-time fraud mitigation tools, “Day 2” tools are still the predominate resource in the industry. These legacy systems operate in “batch” mode. And even the best of the real-time tools typically require someone to manually review and decision some portion of the exception/suspect item. In many instances, this involves reaching out to the other FIs, businesses and consumers to verify. This requires time that must be considered with a faster payments system.
- **f.** Another item to consider is the cost of expediting payments and settlement of payments. With a compressed time frame to detect, investigate, disposition fraud monitoring alerts as well as claim management, operational and fraud costs are expected to increase.
- **g.** A final operational risk for consideration is the actual dollar limits of the transactions. There may be consideration, as seen in the U.K., for limiting dollar amounts that may be transferred in a period of time until the capabilities to detect fraud and account takeover compromises occurs in real time.

Conclusion:

Payments in the U.S. will continue to evolve as consumers and businesses look for innovative ways to improve customer experiences. There is a need to ensure appropriate levels of risk management and fraud prevention are included in the design of these innovative payment solutions. Early Warning welcomes and encourages industry collaboration and innovation to improve the system and enhance the customer experience, but it also believes proactive attention to new vulnerabilities need to be considered as well in order to protect institutions and the consumers they serve.

About the Author:

Laura Weinflash is Vice President of Product Management for Early Warning and has been with the company since 1999. Prior to joining Early Warning, Ms. Weinflash worked for Bank One Corporation (now part of JPMorgan Chase) for 11 years, serving in a variety of executive roles. She frequently speaks at financial services industry events and regularly quoted in industry publications, including American Banker and Credit Union Times.

About Early Warning - Early Warning provides innovative risk management solutions to a diverse network of 900 financial institutions, government entities and payment companies, enabling businesses and consumers to transact with safety, speed, and convenience. Owned and governed by five of the largest banks in the United States, this unique business model facilitates a data exchange system based on collaborative intelligence and trusted exchange. For more information please visit www.earlywarning.com