FFIEC GUIDELINES

LAYERED SECURITY: HOW MUCH IS ENOUGH?

DEBBIE PEACE, AAP

The guidance says layered security is characterized by the use of different controls at different points in a transaction process. Nine specific methods are cited by the guidance as effective controls that may be included in a layered security program. The guidance is clear not to "limit" it to those nine and even goes on to make additional recommendations.

Q: How many controls are enough and what do the examiners expect?

A: Within the guidance, after the 9 effective controls are cited, page 5, the Agencies expectations are made clear. It states: The Agencies expect that an institution's layered security program will contain the following two elements, at a minimum.

DETECT & RESPOND TO SUSPICIOUS ACTIVITY

The guideline also says that layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:

- Initial login and authentication of customers requesting access to the institution's electronic banking system; and
- Initiation of electronic transactions involving ***the transfer of funds to other parties***

The guidance is clear that the financial institution is responsible for developing processes to detect suspicious activity involving the movement of funds to other parties. Given the fact that the guidance cites the use of positive pay, debit blocks and other techniques to appropriately limit the transaction use of an account, out-bound ACH and wire transfers are not the only types of transactions to be considered. Unauthorized incoming ACH debits to a business account that go undetected, ultimately result in transfer of the business customer's funds to another party and loss of confidence, even when funds are recovered.

Stronger authentication methods will certainly help tighten access to the online channel but at the end of the day, ensuring funds cannot be taken, undetected, from an account is the problem the industry is trying to solve.

DETECT AND RESPOND

DOES THIS MEAN FINANCIAL INSTITUTIONS HAVE THE RESPONSIBILITY TO DETECT AND RESPOND TO SUSPICIOUS ACTIVITY?

If your financial institution assumes the responsibility to detect and respond to suspicious activity for your clients, can you really hold them accountable if a loss occurs?

The first effective control mentioned in the FFIEC Guidelines to be included in a layered security program is *"fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response."* Does this mean the guidance is suggesting financial institutions assume responsibility for detecting and responding to suspicious activity **on behalf of their customers**?

This guidance is clearly placing responsibility on financial institutions to implement layered security controls that include **processes designed to detect anomalies and effectively respond to suspicious or anomalous activity**. Thus financial institutions are left to determine what constitutes an anomaly, the best method to detect it and the most effective way to enable a timely response.

SO WHAT CONSTITUTES ANOMALY?

The definition of anomaly is something that deviates from what is standard, normal or expected. Financial institutions can invest in and build complex rules for behavioral monitoring systems to detect transaction anomalies as well as assuming the responsibility of analyzing each anomaly to determine when a financial institution response is merited.

IS THIS REALLY THE BEST APPROACH?

From the customer's perspective, if the financial institution assumes responsibility the customer is more than willing to let them do it. What happens if the financial institution misses something or fails to respond in a timely manner?

WHO IS ACCOUNTABLE FOR THE LOSS?

Let's say a financial institution chooses a behavioral-based monitoring system and/or assume responsibility for securing the browser session or blocking the IP addresses. Then a fraudster "breaks in" and initiates a fraudulent ACH or wire transaction within the normal and expected limits and time window and it isn't detected.

WHO IS RESPONSIBLE FOR FAILING TO DETECT THE ANOMALY?

Should financial institutions really make customers responsible for detecting and responding anomalies? This should ***not*** be avoided. While financial institutions are typically hesitant to have their customers submit to another inconvenient process, in reality, the customer is the only one that can best determine if movement of funds is or is not fraudulent. After all, the customer is in possession of the valid payment information details for the companies or employees they pay and the customer knows who is authorized to debit their account.

Contrary to a behavioral-based approach, financial institutions should **consider a detection and response strategy that systematically monitors where a client's funds are going and who is trying to pull funds from a client's account, based on the client's instructions**. And if an anomaly is detected, the financial institution can leverage advances in communications technology like SMS text to send an out-of-band alert to a separate access device to prompt the customer to review and securely respond to the anomaly within a specific time window.

In the scenario described above, the financial institutions will have satisfied the FFIEC guidance to detect suspicious activity and effectively shift the responsibility to the customer to respond in a timely manner; and now the financial institutions' effective responses to process or not process the transactions will be based on the customers' instructions.

ENLISTING CLIENT PARTICIPATION

SO IF THE CUSTOMER AUTHORIZES THE FUNDS TO BE MOVED TO AN UNAUTHORIZED PARTY, WHO IS RESPONSIBLE?

The role customers will play in a financial institution achieving FFIEC compliance objectives will be solely driven by the financial institution. For financial institutions that continue to offer customers online access to move funds and take on the responsibility of detecting and responding to anomalies on behalf of their clients, their customer will take on no role at all. The cost of compliance and quite possibly the responsibility for losses will fall squarely on the shoulders of those financial institutions. **However, financial institutions that enlist their client's participation to comply with the guidance will reduce operating expense, shift liability, strengthen customer relationships and tap into a lucrative revenue opportunity.**

Perhaps you have made statements like: *"My customers won't even use positive pay today." "My customers won't leverage the ACH debit blocks and filters we already offer."* These are valid statements we have heard many times from financial institutions when they are presented with a solution that requires customer involvement to prevent ACH and wire transaction fraud. *"We don't want to inconvenience our customers."* is another concern we have heard.

CHECK POSITIVE PAY AND ACH DEBIT FILTERS

Let's explore check positive pay and ACH debit filters. No wonder customer adoption is low. For check positive pay, the customer is generally required to submit a file to the financial institution each and every time checks are issued so the financial institution can match check numbers and payee name information to the face of the check when it's presented for payment. This involves file exporting, formatting and file transmission capabilities that most medium- to small-sized business systems are not easily equipped to do.

ACH debit filters are even worse. This process typically involves a customer placing a complete ACH debit block on their account and then if they want to allow a company to debit their account, they must obtain the Company ID from the company debiting them that will appear in the batch header record of the ACH file and give that to the financial institution to set it up in a system, in advance. If you have individuals at both organizations that have AAP or CTP accreditation or some knowledge of ACH, it's probably not an issue but if not, it can be a bit complicated for most people.

CONVENIENCE AND REAL-TIME CONTROL

IF THE PROCESS WERE MORE CONVENIENT AND CONDUCTED IN REAL TIME, WOULD CUSTOMERS WANT THE PROTECTION THESE AND OTHER FRAUD PREVENTION TOOLS ARE DESIGNED TO PROVIDE?

The fact some customers are willing to use the antiquated methods mentioned and even pay for them suggests that by simplifying and automating the fraud detection, response and dispute process, financial institutions could tap into a new residual-recurring revenue stream.

Financial institutions that respond to the FFIEC guidance by wisely investing in scalable technology to allow them to reduce operational task:

1) shift responsibility to the customer by providing the customer with a self-service model that can be offered to a broader base of "paying customers," and
2) position themselves light years ahead of their competitors

The marketing approach financial institutions use to promote fraud prevention solutions to their clients will be the key to customer adoption and revenue generation. Instead of being afraid to inform the customer of the inherent risk to wire and ACH transactions, boldly inform them of the risks that exist outside your financial institution and how those risks can negatively affect them. Offer your customers a convenient service that empowers them to validate inbound and outbound electronic transactions before funds leave their account.

CONVENIENCE IS APPEALING TO CUSTOMERS BUT REAL-TIME CONTROL TAKES THE FINANCIAL INSTITUTION'S MARKETABLE OPPORTUNITY TO A WHOLE NEW LEVEL.

Customers like control; isn't that evident in the fact that most businesses still pay by check?

Financial institutions need a strategy to deliver the message positively and in a variety of venues. Written communication is one method, though ignored by most customers. Financial institutions should ask customers face to face. Present them the risks. Share the best practices with customers including technology solutions available through their financial institution. Other promotional tools for customers include short video presentations that can be streamed over the financial institution's website or through social media sites.

Every financial institution must address fraud and regulatory compliance. How financial institutions address it will determine their legal liability, staffing requirements, customer perception and the impact to their bottom line.