Panel: Member Portal Frauds and Fraud Prevention

Questions:

1. Describe any breach or fraud relating to your member web portal at your fund.
2. What was your incident response process and did it work well?
3. How was internal audit involved in the incident response process?
4. What controls has your organization put in place to prevent future breaches/web portal frauds?
5. Are you using any third parties as part of your controls such as Experian?
6. What controls did you consider but not put in place and why?
7. What audit work have you done to validate the controls?

GENERAL CONTROLS

Ref	Control	Value	Pros	Cons
G-1	Monitor IP Risk Rating	Moderate	This control will monitor and evaluate the IP addresses that access the on-line account and provide a risk ranking based on characteristics of the IP address.	It is time consuming to review the risk report to look for suspicious activity. Many false positives.
G-2	Geo-blocking using Geolocation – Block access to IP addresses from outside the country or from specific countries	Moderate	This control reduces the population of devices that can access the website and can prevent access by potential hackers.	This control is arbitrary and makes assumptions about a broad range of users. It would block legitimate users who are vacationing or who have retired to foreign countries.
G-3	Use geo-fencing to block access from incompatible locations. For example, a legitimate member logs in from New York and then an hour later a fraudster logs in from California. The member could not have gotten to California in one hour so the second login is blocked.	Weak	This blocks unusual activity for review.	The likelihood of a legitimate member and a fraudster attempting to access the same account within a short timeframe is so low the control is not likely to generate many hits. This control is arbitrary and makes assumptions about a broad range of users. It would block legitimate users who are traveling or who have shared their credentials with a trusted family member for help. Also, travel time between locations can vary considerably. How much time do you allocate between locations; the minimum, the average or the maximum? Users often show different geolocations when they switch between machines and cellphones. The IP address used by your phone

				comes from a pool owned by your carrier and may or may not be registered somewhere near your location. This can produce false positives
G-4	Mask sensitive data – masking sensitive data on display screens within an account (e.g., bank account numbers, Social Security number, birthdates, etc.)	Moderate	This is a good control to prevent a fraudster from gathering more information about a member if unauthorized access is gained.	This prevents a legitimate user from verifying whether or not the retirement system has captured and recorded the correct information.

CONTROLS OVER NEW ACCOUNTS

Ref	Control	Value	Pros	Cons
N-1	Waiting period before member can effect transactions (e.g., 5 days)	Weak	Might frustrate a hacker who wants to get in and get out quickly.	By itself this is not a very effective control.
N-2	Send a negative Confirmation of account opening to postal address of record	Moderate	Alerts member that an on-line account has been opened. If the member did not open the account they can call the Retirement System to disable the account. This control is stronger in conjunction with a waiting period (Control N-1) to allow the member to react.	No response from the member assumes the member opened the account; however, many members do not read this kind of mail or may be away from home; especially retirees. This reduces the value of the control.
N-3	Send a positive Confirmation of account opening with security code to postal address of record	Strong – It is unlikely that the thief will have access to the necessary member PII and also be present to retrieve the physical confirmation letter to obtain the security code.	Alerts member that an on-line account has been opened and requires them to log into the new account and enter a security code provided to them in the letter. If the member did not open the account they can call the	May be perceived as a customer service inconvenience because it causes the member an additional step.

			Retirement System to disable the account. This is similar to activating a new credit card and members should be familiar with the process.	
N-4	Challenge questions - Verification to original records in the retirement system's databases. For example: What was the name of your first employer with this retirement system?	Moderate	This approach can help validate a genuine member with information not commonly stolen and used for identity theft.	Slight variations to the answer to a challenge question could cause a rejection and frustration for the bona fide member. For example, if the retirement system's records indicate that the member first worked at "Any Town City School District" and the member answers "Any Town Schools" a rejection could occur. To avoid this, the retirement system would have to employ some sort of "fuzzy logic" to match similar, but not exact, entries.
N-5	Challenge questions – Verification to public records. For example: Which of these cars have you owned [multiple choices]?	Moderate	This approach can help validate a genuine member with information not commonly stolen and used for identity theft.	Cost. Also, the strength applied to the questions might even cause a valid member to answer incorrectly. A lower level of strength might not provide much additional control.
N-6	Use retirement system member number as one of the identifiers for member registration v. Social Security Number.	Moderate	This approach can help validate a genuine member with information not commonly stolen and used for identity theft.	Because the retirement system member number is only used at the retirement system and because pensions are a long-term passive benefit, which members don't necessarily access frequently, even the members don't know their member number offhand.

CONTROLS OVER EXISTING ACCOUNTS

Ref	Control	Value	Pros	Cons
E-1	Password Strength - Member portal logins should contain the same strength requirements as the retirement system's network access. Enforced policies should address length of the password, and the use of varied characters (upper case letters, lower case letters, numbers and special characters).	Moderate	Strong passwords are the first line of defense in preventing unauthorized access.	Customer service complaints and maintenance to reset passwords.
E-2	Account lockout after multiple failed login attempts (e.g., 5 attempts)	Moderate	This is a standard control to prevent a fraudster from simply guessing a member's password.	Customer service complaints and maintenance to reset passwords.
E-3	Account logout after a period of inactivity (e.g., 10 minutes)	Moderate	This is a standard control to prevent a subsequent unauthorized user from continuing a legitimate on-line session.	Customer complaints if the logout interval is too short.
E-4	Multi-factor authentication – PIN sent to email	Moderate	Would prevent a fraudster from gaining access to an account by only intercepting the account credentials.	If a fraudster successfully perpetrates an identity theft, and steals a member's account credentials, they may also have stolen email credentials and would be able to retrieve the PIN from the second factor authentication.
E-5	Multi-factor authentication – PIN sent to phone via text or voicemail	Strong	Would prevent a fraudster from gaining access to an account by only intercepting the account credentials. This is stronger than sending the PIN to the member's email, because it is less likely that the member's phone would also be	

			compromised. This also offers better protection from theft by an ex-spouse, who may have knowledge of the member's PII and account credentials, because the ex-spouse is not likely to have access to the member's phone.	
E-6	Send a negative Confirmation of transaction to postal address of record	Moderate	Alerts member that an on-line transaction has occurred. If the member did not effect the transaction they can call the Retirement System to cancel it. This control is stronger in conjunction with a waiting period (Control N-1)	No response from the member assumes the member effected the transaction; however, many members do not read this kind of mail or may be away from home; especially retirees. This reduces the value of the control.
E-7	Send a positive Confirmation of transaction with security code to postal address of record	Strong – It is unlikely that the thief will have access to the necessary member PII and also be present to retrieve the physical confirmation letter to obtain the security code.	Alerts member that an on-line transaction has occurred and requires them to log into the new account and enter a security code provided to them in the letter. If the member did not effect the transaction they can call the Retirement System to cancel it. This is similar to activating a new credit card and members should be familiar with the process.	May be perceived as a customer service inconvenience because it causes the member an additional step.
E-8	Challenge questions (personal) - Ask challenge questions when effecting a transaction. For example, even if a member is successfully logged in, when they attempt to change the bank account, ask them a pre-determined question (What street did you grow up on?)	Moderate	This is a good secondary control because it validates the member with a question that is personal to them but is not based on PII that is frequently stolen.	Customer service.

E-9	Challenge questions (prior information) - Ask challenge questions when effecting a transaction. For example, even if a member is successfully logged in, when they attempt to change the bank account, ask them to enter the previous account number.	Moderate	This is a good secondary control because it validates the member with a question that they should know but is not based on PII that is frequently stolen. This control is only effective if sensitive data is masked within the account (Control G-4).	Customer service.
E-10	User imposed restriction on account functionality. Allow the user to deactivate self-service features. For example, a member may want a self-service account to monitor certain activity (read only) but deactivate the ability to effect transactions (e.g., change bank accounts).	Moderate	This could prevent a fraudster from effecting transactions during an account takeover.	Depends on user diligence to deactivate unneeded services. If the fraudster has the ability to take over the account, they may also have the ability to remove the restrictions while posing as the user. Overhead - Requires an additional level of security to access the account functionality pages.
E-11	Deactivate dormant accounts (e.g., accounts that have not been accessed in 3 years).	Moderate	This control removes dormant accounts from service, which are an attractive target for fraudsters because the account owner is less likely to notice the additional activity.	Because of their long-term nature, pension accounts are accessed less frequently than, say bank accounts, leading to customer service complaints from members who access their accounts infrequently and have to set up a new account each time.
E-12	Provide a “landing page” when the member enters their account that informs them of the time and date of their last login.	Moderate	This can alert the member to fraudulent activity if they did not initiate the last session appearing on the landing page.	Members may not pay attention to the information on the landing page or may not remember their last login.