CYBER SECURITY Newsletter

RED FLAG RULES

Problem

The Red Flags Rule is a federal regulation requiring organizations to implement an Identity Theft Prevention Program designed to detect the warning signs, or red flags, of identity theft. An Identity Theft Prevention Program is a playbook which includes reasonable policies and procedures for detecting, preventing and mitigating identity theft. By identifying red flags in advance, we can spot suspicious patterns and take appropriate steps to prevent identity theft from happening.

Identity theft is a fraud committed or attempted using the identifying information about another person without their authority. Identifying information is anything that can be used to identify a specific person, including their name, social security number, date of birth or employer identification number.

So, what should you be looking for? Some of the most common red flags for identity theft include but are not limited to the following:

- Documents provided for identification or an application appears to have been altered or forged.

- The photograph or physical description on the identification is not consistent with the appearance of the applicant presenting the identification.

- The Social Security Number has not been issued, is listed on the Social Security Administration's Death Master File, or is the same as that submitted by other persons opening an account or other customers.

Red Flag Rules

This is a federal regulation our organization is required by law to follow. It is designed to detect warning signs (called Red Flags) of identity theft. You are required to look for and report any of these indications of identity theft.

JUNIATA COLLEGE

This newsletter is published by Campus Technology Services. For more information please contact us at:
help@juniata.edu

Pretexting

One of the key provisions of RFR involves pretexting. Pretexting is when someone pretends to be someone or something else to get information illegally (also often called social engineering). These attacks can come in a variety of forms, such as a phishing email that pretends to come from a bank or a criminal calling people and pretending to be their credit card company. In addition, criminals or other unauthorized people can contact our organization pretending to be one of our customers. This is often a very effective way for an attacker or criminal to gain access to someone else's identifying information.

This is why we have strong processes and procedures in place to first verify the identity of all customers before discussing any private information. Always follow these processes. If you are contacted by any individual whom you believe is attempting a pretexting (or social engineering) attack, please contact your security team immediately.

- The phone number is invalid, or is associated with a pager or answering service.

- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

- For departments that use challenge questions, the person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns.

- An account is used in a manner that is not consistent with established patterns of activity on the account.

- A material change in telephone call patterns in connection with a cellular phone account.

- An account that has been inactive for a reasonably lengthy period of time is suddenly used.

- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

- Our organization is notified of unauthorized charges or transactions in connection with a customer's account.

- Our organization is notified by a law enforcement authority or any other person that it has opened a fraudulent account for a person engaged in identity theft.

If you find any of these Red Flags when handling customer financial information, please report it immediately to your security team.