Tips for US Financial Institutions: What to do Post-Breach

Data breaches are a source of risk for financial institutions even at organizations outside of financial institutions. The compromise of personally identifiable information (PII) may increase compliance/regulatory, financial, legal and reputational risks. Below are tips for financial institutions that may help in reducing the impact of data breaches.

Assess Risks to the Institution and Consumer Accounts

The following are common forms of fraud that institutions should consider following an external data breach:

- New account fraud
- Account takeover
- Cash advance fraud
- Online banking and mobile wallet transaction fraud
- Fraudulent wire transfer requests
- Social engineering, phishing and vishing

Leverage Loss Prevention Strategies

A successful loss prevention program includes several of the following components.

Use Fraud Analytic Tools

Behavioral analysis tools can detect suspicious customer or member activity and eliminate false positive alerts through machine learning and algorithms that assess the risk in near-real time of user activity. These tools exist for:

- Credit and debit cards;
- Electronic funds/ ACH transfers;
- Online banking;
- Mobile banking; and
- Checks and other draft instruments.

If your institution does not currently use these tools, identify fraud reporting capabilities from your core or card processing third-party service provider.

Verify New Account Requests

Verify the information of any customers or members requesting to establish a new account relationship. Institutions should follow their *Know Your Customer or Member Identification Procedures* to reduce the risk of new account fraud.

Verify Existing Account Requests

Verify account ownership to identify and authenticate account owners for account funding and account-to-account transfers using one or more of the following methods:

- **Instant verification** validates real customers and improves the customer experience while reducing the opportunity for fraud;
- **Real-time account verification** compares data entered by a user with data collected from the website of the financial institution servicing the account;
- **Trial deposit verification** validates the external account with two small trial deposits while the account holder confirms the amount of the two deposits;
- **Identity verification** provides financial institutions access to multiple third-party data sources and the ability to verify a customer's or member's identity in real-time; or
- **Out of wallet questions** are designed to trick the fraudster by asking more sophisticated questions only the legitimate customer will recognize.

Tips for US Financial Institutions: What to do Post-Breach

Review *Red Flags* Policy and Procedures

After any type of breach that compromises or exposes the PII of consumers, your institution may want to review your *Red Flags* policy and procedures. Determine if there are any additional activities that a criminal could do with the exposed information to stage an account takeover, such as sounding much older or younger than the age on file or asking for information they should already know, to include asking if they have a credit card or the names of account co-signers.

Offer Out-of-Band Verification

Provide a means of authentication requiring two different signals from two different networks or channels.

Offer Two-Factor Authentication via Online and Telephone

Provide authentication methods that involve confirming one or more of three factors:

- Something only the user should know, such as a password or PIN;
- Something the user possesses, such as an ATM card, smart card or token; or
- Something the user is, such as a biometric characteristic like a fingerprint or iris pattern.

Review Authentication Procedures

Be mindful that, with each new breach, secondary methods used to authenticate customers or members for highly sensitive requests may become disclosed and no longer a reliable source of authentication. If current secondary methods include authenticating via an account numbers, portion of a payment card number, address, driver's license number or employment information, consider using optional authentication questions that are likely not stored at an outside vendor, such as the following offered by other FS-ISAC members:

- Branch where the customer or member opened their account;
- Relationship manager, for business accounts;
- Online banking access ID or username (if not SSN);
- Online banking security question;
- Transactional information, such as the date, amount and description, location, merchant name of a deposit, withdrawal, debit card transaction, transfer, ACH/bill pay, fee, check or wire;
- Approximate balance; and
- Any other account-specific questions that only the account holder would know.

Offer Customers/Members *Self-Service* Fraud Detection Options

There are a couple of options an institution may offer consumers to perform *self-service* fraud detection. Educating customers or members on how to set transaction alerts through the online or mobile banking platforms is one option; be sure to tell them what to watch for. Another is to suggest they logon to their online banking access once a day or several times a week, to monitor the activity and transactions.

As well, institutions may select to purchase an application that works with their online or mobile banking platforms that gives customers/members the ability to control the availability of their credit or debit cards. While still in their infancy and usually provided as a mobile app, these tools allow the consumer to "turn off" or "turn on" payment cards tied to their accounts, giving them the power to restrict or allow transactions on a specific card or account.

Provide Security Awareness Training

Teach employees, commercial and retail customers about the different fraud types, how fraudsters use them and what action they should take if they meet suspicious activity. Other options include:

- Fraud assessment that can be shared with commercial customers to identify gaps in their organization;
- Security center on your corporate website;
- Statement stuffer; and
- Branch brochures and signage.

FS-ISAC

Tips for US Financial Institutions: What to do Post-Breach

Safeguard Financial Institution Networks

With each new data breach comes an opportunity to re-assess your institution's internal processes and safeguards, to ensure no new gaps have come up. In that spirit and in addition to the security awareness training indicated above, below are five very brief reminders of actions every institution can take to protect themselves and their customer/member sensitive information.

- Keep a dynamic inventory of the hardware (devices, PCs, servers, etc.) and software (OSes, applications, web apps, mobile apps, etc.) on your network, in order to quickly determine if an update or patch applies in your network;
- Sign up for FS-ISAC, US-CERT and manufacturer alerts to know when a piece of hardware or software has a vulnerability and the update or patch is available; patch immediately, especially if the vulnerability is being exploited; if you cannot patch or no update is available, determine other mitigations to protect the asset;
- Protect sensitive information with appropriate safeguards, such as a firewall, IPS / IDS, proxy, email controls, anti-virus / anti-malware protections, encryption, application whitelisting, data loss prevention actions, etc.;
- Provide safe configurations for hardware and software, to include password protections, privileged account protections, changing default admin passwords, restricting file types from running, etc.;
- Verify the above controls are working as intended by performing regular and routine vulnerability assessments, penetration tests and assessing employees' ability to avoid phishing emails.

Assess and Refine Incident Response and Consumer Notification Procedures

Minimize damage to the institution and its customers through containment of the incident and proper restoration of information systems. A key element of incident response involves assigning responsibility for evaluating, responding and managing security incidents and developing guidelines for employees to follow regarding escalation and reporting procedures.

Verify the Incident Response Lifecycle

- Investigate alerts that appear benign;
- Determine the cause (insider threat, denial of service, malicious code, improper usage, scans, probes, attempted access and incident investigation);
- Contain the incident - Protect and keep available critical computing resources where possible, determine the operational status of the infected computer, system or network;
- Investigate and fact gather - application, network and system logs, copy drives and external storage;
- Eradicate the cause - Get rid of the issue on your computer, system or network. Note: This step should only take place after all external and internal actions are completed;
- Recovery - Restoration of service; and
- Follow-up - Ask questions that should be answered to ensure the process is sufficient and effective.

Notify Consumers

When a financial organization becomes aware of an incident of unauthorized access to sensitive customer information, the organization should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the organization determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. The contents of a breach notification should contain the following elements:

- a general description of the incident and the information that was the subject of unauthorized access;
- a telephone number for further information and assistance;
- a reminder to remain vigilant over the next 12 to 24 months;
- a recommendation that incidents of suspected identity theft be reported promptly; and
- a general description of the steps taken by the financial institution to protect the information from further unauthorized access or use.