**Extion Infotech**

**Project 2**

**Report-2**

**Investigation On Data Breach**

**Flagstar Bank Data Breach**

**Created by: -**

**Krishna Shankar**

**Cybersecurity Intern, Extion Infotech**



**About the Company: -**

Flagstar Bank, a major financial institution in the United States, has faced multiple cybersecurity breaches over the past three years, compromising the personal and financial data of millions of customers. These breaches were linked to third-party vulnerabilities, ransomware attacks, and weaknesses in the bank’s cybersecurity infrastructure.

**Incident Analysis: -**

Incident Title: - **Flagstar Bank Data Breach**

Date of Incident: -December 2021 - Data Breach

Location: - Flagstar Bank, Corporate Drive, Michigan United States of America.

Incident Type: - Data Breach

**1. December 2021 - Data Breach**

* **Date Discovered:** June 2022
* **Affected Individuals:** 1.5 million
* **Data Compromised:** Social Security Numbers (SSNs), banking details, personal information (names, addresses, birthdays)
* **Cause:** Security vulnerability exploited by the Clop ransomware gang
* **Response:** Notified affected individuals and offered 24 months of free identity monitoring

**2. March 2021 - Accellion File Transfer Breach**

* **Affected Individuals:** 1.6 million
* **Data Compromised:** Personal and employee information (names, addresses, phone numbers, tax records, SSNs)
* **Cause:** Clop ransomware gang exploited vulnerabilities in Accellion’s file transfer server
* **Impact:** Affected over 100 organizations globally, including Harvard Business School and the City of Toronto

**3. May 2023 - MOVEit Data Breach via Fiserv**

* **Date of Breach:** May 27 - May 31, 2023
* **Date Discovered:** June 3, 2023
* **Affected Individuals:** 837,390
* **Data Compromised:** Names, Social Security Numbers
* **Cause:** Third-party vulnerability in MOVEit Transfer software used by Fiserv
* **Response:** Notified customers, patched vulnerabilities, and provided identity monitoring

**4. October 2023 - Security Vulnerability Exploit**

* **Affected Individuals:** Unknown
* **Data Compromised:** Personal customer data
* **Cause:** Exploited security vulnerability
* **Response:** Investigation and mitigation efforts

**About the Attacker: -**

The cybercriminals responsible for the **Flagstar Bank data breaches** remain unidentified, but their tactics, techniques, and procedures (TTPs) indicate they were **highly sophisticated attackers**, likely **linked to organized cybercrime groups**. These breaches were **well-coordinated**, **targeted**, and **leveraged multiple attack vectors**, including **zero-day vulnerabilities, supply chain attacks, and ransomware deployment**.

**Possible Attacker Profiles & Their Methods**

**1. Clop Ransomware Gang (2021 Breach)**

* The **first major breach in 2021** was **attributed to the Clop ransomware gang**, a **notorious cybercriminal group** specializing in **exploiting supply chain vulnerabilities** to attack **large enterprises**.
* **Tactics Used**:
  + Exploited **Accellion’s legacy file transfer appliance**, a software known to have **unpatched security flaws**.
  + **Compromised sensitive customer data** before launching the ransomware attack.
  + **Deployed ransomware** across the Flagstar Bank network to encrypt critical systems and demanded a **ransom payment** for data recovery.
  + **Used stolen credentials** to escalate privileges and **move laterally within the bank’s IT infrastructure**.
  + Communicated **ransom demands via fax and email**, an unusual but previously documented **Clop tactic**.

**2. Unidentified Advanced Threat Actor (2023 Breach)**

* The **most recent attack in 2023** targeted **Fiserv**, a third-party **vendor providing financial services** to Flagstar Bank.
* This attack **leveraged a zero-day vulnerability** in **MOVEit Transfer**, a **widely used secure file transfer application**.
* **Tactics Used**:
  + **Exploited the MOVEit zero-day flaw** to gain unauthorized access to **Fiserv’s systems**.
  + **Pivoted from Fiserv’s network** to extract personally identifiable information (**PII**) of **nearly 800,000 Flagstar Bank customers**.
  + Data stolen included **names, Social Security numbers (SSNs), and other sensitive information**.
  + **Used privilege escalation techniques** to bypass security controls and navigate internal networks.
  + **Exfiltrated customer data in multiple stages** to avoid detection by traditional security monitoring systems.
  + The **data theft was carried out before any security patches** were released for the **MOVEit** vulnerability, indicating a **highly coordinated and premeditated attack**.

**Key Observations & Trends in Attack Strategy**

1. **Use of Zero-Day Vulnerabilities**:
   * The attackers capitalized on **previously unknown security flaws** (zero-days), making **traditional cybersecurity defenses ineffective**.
   * Both the **Accellion** and **MOVEit Transfer** breaches demonstrate a **pattern of targeting vulnerable third-party file transfer services**.
2. **Targeting of Supply Chain & Third-Party Vendors**:
   * Instead of attacking **Flagstar Bank directly**, the cybercriminals infiltrated **weaker, less secure third-party service providers** (**Accellion and Fiserv**).
   * This **supply chain attack strategy** allows hackers to gain access to **multiple organizations** that use the same compromised vendor, **multiplying their impact**.
3. **Exfiltration of Sensitive Data Before Ransomware Deployment**:
   * Unlike **traditional ransomware attacks**, where files are encrypted first, these attackers prioritized **stealing sensitive information**.
   * The **2021 Clop breach** and the **2023 MOVEit attack** suggest the data was **exfiltrated in phases** before security teams could detect or respond.
4. **Potential Links to Organized Cybercrime Groups**:
   * Clop ransomware **has been linked to Russian-speaking cybercriminal groups**, often associated with **financially motivated cyberattacks**.
   * The **2023 breach, though unattributed**, shows signs of a **well-funded, highly organized cybercrime operation** with **advanced capabilities**.
   * Given the scale and sophistication, **nation-state actors cannot be ruled out**, although the primary motivation appears to be **financial gain**.

**Summary of the Incident: -**

**Flagstar Bank has suffered three major data breaches since 2021, with the latest occurring in 2023.**

**2023 Breach:**

* **Caused by a security flaw in MOVEit Transfer, a secure file transfer application.**
* **Exploited by hackers through a zero-day vulnerability.**
* **Targeted Fiserv, a third-party vendor used by Flagstar Bank.**
* **Exposed sensitive customer data, including names and SSNs.**
* **Affected approximately 837,390 individuals.**

**2021 Breach:**

* **Linked to the Clop ransomware gang.**
* **Exploited Accellion’s outdated file transfer software.**
* **Exposed data of 1.5 million customers.**

**June 2022 Incident:**

* **Compromised PII (Personally Identifiable Information) of 1.4 million clients.**

**Attack Pattern:**

* **Hackers exploited third-party vendors' weaknesses to infiltrate Flagstar Bank’s systems.**

**Bank’s Response:**

* **Launched forensic investigations into the breaches.**
* **Notified affected individuals about the incidents.**
* **Provided credit monitoring services to mitigate risks.**

**Concerns Raised:**

* **Repeated breaches have raised doubts about Flagstar Bank’s cybersecurity practices.**
* **Questions remain about its ability to protect customer information effectively.**

**Forensic Analysis:**

**Forensic investigations were conducted after each Flagstar Bank data breach to determine:**

* + **Attack vectors used.**
  + **Extent of data exposure.**
  + **Tactics, techniques, and procedures (TTPs) of the attackers.**

**2021 Breach (Clop Ransomware Attack)**

* **Attackers: Attributed to the Clop ransomware gang.**
* **Attack Methodology:**
  + **Exploited Accellion’s outdated file transfer appliance.**
  + **Used stolen credentials to infiltrate Flagstar Bank’s network.**
  + **Deployed ransomware to encrypt files and systems.**
  + **Demanded a ransom payment via fax and email.**
* **Forensic Findings:**
  + **Attackers exfiltrated sensitive customer data before deploying ransomware.**
  + **Lateral movement within the network was detected, likely through privilege escalation techniques.**
  + **Analysts found evidence of data staging (preparing files for extraction before exfiltration).**

**2023 Breach (MOVEit Zero-Day Exploit)**

* **Attackers: Unidentified but used highly sophisticated tactics.**
* **Attack Methodology:**
  + **Exploited a zero-day vulnerability in MOVEit Transfer, a file transfer software used by Fiserv (a third-party vendor).**
  + **Gained unauthorized access to Fiserv’s systems.**
  + **Stole Flagstar customers' PII, including names and Social Security Numbers (SSNs).**
* **Forensic Findings:**
  + **Digital forensics teams analyzed:**
    - **Server logs to track unauthorized access.**
    - **Network traffic to detect malicious data exfiltration.**
    - **Compromised accounts used for escalation and persistence.**
  + **Hackers utilized privilege escalation to gain deeper access and move laterally across Fiserv and Flagstar Bank’s interconnected systems.**
  + **Evidence suggested that stolen data was exfiltrated in multiple stages, likely to avoid detection.**
  + **It remains unclear whether all stolen data was deleted after ransom payments, raising concerns about future misuse.**

**Challenges & Additional Investigations**

* **Delayed Dark Web Monitoring:**
  + **The risk advisory firm Kroll conducted a dark web analysis to check if stolen data was being sold.**
  + **However, monitoring only began 10 months after the breach, limiting its effectiveness in preventing identity theft.**
* **Unanswered Questions:**
  + **Whether all exfiltrated data was recovered or permanently deleted.**
  + **Potential collaboration between attackers and insider threats (not ruled out).**
  + **Flagstar Bank’s vulnerability management failures, given the repeated breaches through third-party vendors.**

**These findings highlight serious security lapses in Flagstar Bank’s vendor management, network monitoring, and response strategies, raising concerns about the bank's ability to prevent future attacks.**

**Conclusion**

The Flagstar Bank data breaches highlight a critical vulnerability within the financial sector, emphasizing the increasing sophistication of cyberattacks. These incidents underscore the importance of robust cybersecurity measures, especially in safeguarding against supply chain risks and leveraging defenses against zero-day exploits. The attackers' advanced tactics reflect a concerning trend in the cyber threat landscape, where highly skilled adversaries target strategic points within financial systems. As such, financial institutions must adopt proactive, comprehensive security strategies and continuously evolve their defenses to counteract the growing threat posed by cybercriminal groups, ensuring the protection of sensitive customer data and maintaining trust within the sector.

**The Attackers Behind the Flagstar Bank Data Breaches**

**The attackers responsible for the Flagstar Bank data breaches remain unidentified, but their methodologies suggest they were sophisticated cybercriminals with potential links to organized cybercrime groups. The breaches leveraged multiple attack vectors, including zero-day vulnerabilities, ransomware, and supply chain attacks, indicating a high level of expertise in exploiting enterprise-level security flaws.**

**2021 Breach: Clop Ransomware Gang**

* **The Clop ransomware gang, a Russian-speaking cybercriminal group, is known for targeting large organizations through supply chain vulnerabilities.**
* **Attackers exploited Accellion’s legacy File Transfer Appliance (FTA), an outdated software used for secure file sharing.**
* **This vulnerability enabled unauthorized access to sensitive Flagstar Bank customer data.**
* **The gang exfiltrated large volumes of personally identifiable information (PII), including Social Security numbers (SSNs), financial records, and contact details.**
* **The stolen data was used for extortion, with ransom demands issued via fax and email, a rare but strategic move to bypass email security filters.**

**2022 Breach: Possible Reuse of Stolen Credentials**

* **The June 2022 breach affected 1.4 million customers, though details about the attackers remain unclear.**
* **Cybersecurity experts suggest the incident may have involved stolen credentials, potentially acquired from previous breaches or dark web marketplaces.**
* **The breach reinforced concerns about inadequate security controls at Flagstar Bank, particularly in managing third-party vendors.**

**2023 Breach: MOVEit Zero-Day Exploit**

* **The 2023 attack targeted Fiserv, a third-party service provider for Flagstar Bank, using a zero-day vulnerability in MOVEit Transfer, a widely used secure file transfer application.**
* **The attackers bypassed authentication mechanisms, gaining unauthorized access to systems and exfiltrating data.**
* **The stolen data included names, SSNs, financial details, and other PII, impacting 837,390 customers.**
* **The incident followed a growing trend of cybercriminals attacking financial institutions through third-party supply chains, where security measures are often weaker.**

**Attack Tactics and Techniques Used**

* **Zero-Day Exploitation: Attackers took advantage of unpatched vulnerabilities in widely used software, ensuring maximum impact before detection.**
* **Supply Chain Attacks: Instead of directly breaching Flagstar Bank, hackers compromised third-party vendors (Accellion and Fiserv) to infiltrate Flagstar’s systems.**
* **Privilege Escalation: Once inside, attackers gained higher-level access to move laterally across networks and extract large volumes of sensitive data.**
* **Data Exfiltration & Ransomware: Stolen data was either encrypted for ransom demands or sold on dark web forums to maximize financial gain.**
* **Use of Advanced Persistent Threat (APT) Techniques: The long-term infiltration strategy and exploitation of enterprise security gaps suggest involvement from well-funded cybercriminal syndicates or nation-state-backed actors.**

**Possible Threat Actors**

* **Clop Ransomware Gang: Responsible for the 2021 breach, Clop is known for sophisticated extortion tactics, particularly targeting financial institutions and healthcare organizations.**
* **Russian and Eastern European Cybercrime Groups: Many ransomware gangs operate from Russia and neighboring countries, taking advantage of jurisdictional protection from prosecution.**
* **Dark Web Marketplaces: Even if the original attackers remain unidentified, stolen Flagstar Bank data was likely sold on cybercrime forums, enabling subsequent attacks.**

**Implications for Future Threats**

* **Financial institutions are high-value targets, making them attractive to cybercriminals.**
* **Third-party vendor weaknesses remain a critical security risk, as seen in multiple breaches.**
* **Without enhanced security measures, repeat attacks are likely to occur, further compromising customer trust and data integrity.**

**Key Attackers and Their Methodologies: -**

**1. Clop Ransomware Gang (2021 Breach)**

The **Clop ransomware group**, a well-known cybercriminal organization based in **Russia or Eastern Europe**, was attributed to the **2021 Flagstar Bank breach**. Clop specializes in **targeting financial institutions, healthcare systems, and corporations**, primarily through **supply chain vulnerabilities**.

**Tactics Used in the 2021 Breach:**

* **Exploitation of Accellion’s Legacy File Transfer Appliance (FTA)**
  + Accellion's **file transfer software** was outdated and had known vulnerabilities.
  + Clop exploited these weaknesses to gain **unauthorized access** to Flagstar Bank’s **internal systems**.
* **Data Exfiltration & Ransomware Deployment**
  + The attackers extracted **sensitive customer data** (including **SSNs, banking details, and personal identifiers**).
  + Instead of encrypting Flagstar’s data on-site, Clop **exfiltrated** the information and used it for **double extortion**—threatening to **leak the data** unless a ransom was paid.
* **Unconventional Ransom Demands**
  + Clop sent ransom demands via **fax and email**, an unusual method likely designed to bypass **email security filters**.
  + The gang also leveraged **dark web forums** to auction off stolen data for further profit.

**2. June 2022 Breach – Potential Stolen Credential Exploit**

The **June 2022 breach**, which impacted **1.4 million customers**, remains **less documented** than the other incidents. While no single cybercriminal group was explicitly blamed, cybersecurity analysts suspect it may have resulted from **stolen credentials**.

**Possible Tactics Used in 2022:**

* **Reuse of Credentials from Previous Breaches**
  + Cybercriminals may have acquired **login credentials from the 2021 breach**, either through **dark web marketplaces** or internal insider threats.
* **Credential Stuffing Attacks**
  + Attackers used automated tools to test **compromised usernames and passwords** across different systems to gain unauthorized access.
* **Weak Multi-Factor Authentication (MFA) Implementation**
  + If Flagstar Bank had **inconsistent MFA enforcement**, attackers could have bypassed standard security controls.

**3. 2023 Breach – MOVEit Zero-Day Exploit**

The **2023 breach** was significantly more advanced, targeting **Fiserv**, a **third-party service provider** for Flagstar Bank. The attack leveraged a **zero-day vulnerability** in the widely used **MOVEit Transfer software**, a secure file-sharing tool used by financial institutions worldwide.

**Tactics Used in the 2023 Breach:**

* **Zero-Day Exploitation in MOVEit Transfer**
  + A **previously unknown vulnerability** in MOVEit Transfer allowed attackers to bypass **authentication** and execute **malicious code** on Fiserv’s servers.
* **Supply Chain Attack Strategy**
  + Instead of attacking Flagstar Bank directly, the hackers **infiltrated Fiserv**, which had access to sensitive **customer banking data**.
  + This approach enabled **stealthy access** to highly confidential records **without triggering Flagstar’s primary security defenses**.
* **Massive Data Exfiltration**
  + Attackers stole **personally identifiable information (PII)**, including **names, Social Security numbers, financial details, and banking credentials**.
  + Nearly **837,390 customers** were affected by this breach.

**Attackers' Advanced Techniques and Tools**

The **repeated breaches** at Flagstar Bank highlight the **evolving nature of cybercriminal tactics**. Some of the **key attack methods** used across all three breaches include:

**1. Zero-Day Exploits & Supply Chain Attacks**

* Attackers actively **scanned for vulnerabilities** in third-party software (e.g., Accellion, MOVEit) before patches were available.
* They leveraged **supply chain weaknesses** to gain indirect access to Flagstar Bank’s systems.

**2. Ransomware & Double Extortion**

* Instead of simply encrypting Flagstar’s data, cybercriminals **exfiltrated information** first and **threatened public exposure** if the ransom was unpaid.
* Stolen data was **leaked on dark web marketplaces**, leading to identity theft and fraud risks for affected customers.

**3. Credential Theft & Privilege Escalation**

* Cybercriminals likely used **phishing, social engineering, and credential stuffing attacks** to obtain employee or customer login details.
* Once inside the system, they **elevated their privileges** to access sensitive databases.

**4. Lateral Movement & Stealthy Persistence**

* Attackers moved **laterally across Flagstar’s internal network**, evading detection for extended periods.
* They planted **backdoors and remote access tools** to maintain long-term access.

**Potential Attribution & Future Threats: -**

Although the **exact identities** of the 2022 and 2023 attackers remain **unknown**, cyber experts believe they could be associated with:

* **Clop Ransomware Gang** (responsible for the **2021 breach**).
* **Russian or Eastern European Cybercrime Syndicates** leveraging **stolen banking credentials**.
* **Dark Web Threat Actors** purchasing exfiltrated **Flagstar customer data** for **identity theft and financial fraud**.

The **financial sector** remains a **prime target** for cybercriminals due to its **valuable data and critical infrastructure**. Without significant cybersecurity improvements, **Flagstar Bank** and similar institutions remain **vulnerable to further attacks**.

**Post-Incident Review: -**

* **Comprehensive Assessment:**
  + Conduct a **detailed forensic analysis** after each breach to examine **attack vectors, vulnerabilities, and security lapses**.
  + Identify the **root causes** of the attack and document critical lessons learned.
* **Security Audits & Compliance Checks:**
  + Mandate **independent third-party security audits** to assess compliance with **financial industry cybersecurity standards**.
  + Implement **continuous risk assessments** to detect and mitigate potential weaknesses.
* **Incident Response & Preparedness:**
  + Conduct **regular tabletop exercises and simulated cyberattack drills** to train employees on effective response strategies.
  + Update **incident response protocols** based on findings from past breaches.
* **Collaboration with Authorities & Cybersecurity Experts:**
  + Work closely with **law enforcement agencies, cybersecurity firms, and threat intelligence organizations** to track attackers and prevent future breaches.
  + Share threat intelligence with other financial institutions to **strengthen collective defense**.
* **Investment in Advanced Cybersecurity Technologies:**
  + Adopt a **Zero-Trust Architecture (ZTA)** to limit access and prevent lateral movement by attackers.
  + Explore **blockchain-based security solutions** for securing sensitive transactions and customer data.
  + Deploy **AI-driven threat detection** and **automated response mechanisms** to enhance real-time monitoring.
* **Enhanced Data Protection Policies:**
  + Strengthen **encryption standards** for data at rest and in transit.
  + Implement **stricter access controls** and multi-factor authentication (MFA) across all systems.

By implementing these measures, **Flagstar Bank** can **strengthen its cybersecurity posture**, prevent future breaches, and rebuild customer trust.

**Lessons Learned: -**

* **Stronger Third-Party Security Controls:**
  + Ensure **all vendors and third-party partners** comply with **strict cybersecurity policies** to prevent **supply chain attacks**.
  + Regularly **audit third-party security practices** and require compliance with **financial industry security standards**.
* **Timely Incident Detection and Response:**
  + Deploy **real-time security monitoring** and **advanced threat detection systems** to identify breaches at early stages.
  + Establish a **rapid breach response protocol** to minimize the impact of cyberattacks.
* **Comprehensive Data Encryption:**
  + Encrypt **all sensitive customer data** both **at rest and in transit** to reduce exposure risks.
  + Use **tokenization techniques** to protect high-value financial data.
* **Employee Cybersecurity Training:**
  + Conduct **regular security awareness training** to educate employees on **phishing, credential theft, and ransomware tactics**.
  + Implement **strict access controls** and enforce **multi-factor authentication (MFA)** to prevent unauthorized access.
* **Regular Security Audits and Penetration Testing:**
  + Perform **frequent security audits and penetration testing** to identify and mitigate vulnerabilities before attackers exploit them.
  + Continuously update security policies based on evolving **cyber threats and attack trends**.
* **Proactive Dark Web Monitoring:**
  + Continuously monitor **dark web forums and marketplaces** for leaked customer data.
  + Work with **threat intelligence teams** to swiftly respond to data leaks and prevent identity theft.
* **Regulatory Compliance and Transparency:**
  + Ensure **timely reporting** of security incidents to **federal agencies and regulatory bodies**.
  + Maintain **transparent communication** with affected customers, providing **timely updates and mitigation support**.

By integrating these **key lessons**, **Flagstar Bank** can **enhance its cybersecurity resilience**, protect customer data, and prevent future cyberattacks.

**Technical Analysis of Attacks:**

* Attacks involved a combination of zero-day vulnerabilities and credential theft.
* MOVEit vulnerability allowed remote execution of arbitrary code, bypassing authentication, and granting privileged access to sensitive data.
* Accellion breach exploited outdated file transfer software with known security flaws.
* Attackers used lateral movement techniques to access critical systems and exfiltrate customer data.
* Emphasized the importance of regular security audits and prompt patching of third-party applications.

**Impact on Customers and Financial Losses:**

* Heightened risks of identity theft and financial fraud for affected customers.
* Stolen Social Security Numbers and tax records used for fraudulent activities such as loan applications and tax fraud.
* Customers reported incidents of credit card fraud and unauthorized transactions.
* Flagstar Bank faced reputational damage, significant financial losses, legal settlements, increased security costs, and regulatory fines.
* Estimated total cost of breaches exceeded tens of millions of dollars.

**Legal and Regulatory Consequences:**

* Faced multiple class-action lawsuits from affected customers demanding compensation and cybersecurity improvements.
* Investigations conducted by regulatory bodies, including the Office of the Comptroller of the Currency (OCC) and the Federal Trade Commission (FTC).
* Identified compliance violations leading to monetary penalties and stricter oversight.
* Triggered revisions in federal banking cybersecurity regulations, emphasizing third-party risk management.

**Response Strategies and Industry Best Practices:**

* **Cybersecurity Enhancements Implemented:**
  + Enhanced multi-factor authentication (MFA) for all critical systems.
  + Stricter vendor security assessment procedures before integrating third-party services.
  + Real-time threat monitoring and rapid response mechanisms.
  + Encryption of sensitive customer data in transit and at rest.
  + Cybersecurity awareness training for employees and customers to prevent phishing and social engineering attacks.
* **Industry-Wide Best Practices Adopted:**
  + Zero-trust architecture implementation.
  + AI-driven threat detection systems.
  + Mandatory security audits for third-party vendors.

**Communications and Notification:**

* Customers were notified via direct mail regarding breaches.
* In response to the 2023 breach, Flagstar worked with Fiserv to inform customers and provide support.
* Delay in 2022 breach notification (six months) raised transparency concerns.
* Provided impacted customers with two years of free credit monitoring and fraud consultation services through Kroll.

**Post-Incident Review:**

* Exposed critical weaknesses in Flagstar Bank’s third-party vendor security.
* Engaged risk advisory firm Kroll to monitor the dark web for leaked customer data (delayed response noted).
* Recurring breaches highlighted significant gaps in vendor risk management.
* Customers filed class-action lawsuits seeking damages and cybersecurity improvements.
* Federal authorities emphasized the need for stricter supply chain security controls.

**Lessons Learned:**

* Strengthen third-party risk assessment and enforce stricter vendor security requirements.
* Implement real-time monitoring and rapid response mechanisms to detect cyber threats.
* Enhance encryption and multi-factor authentication for better protection of sensitive data.
* Educate employees and customers about cybersecurity threats like phishing and ransomware attacks.
* Ensure timely and transparent communication with affected individuals to maintain trust and mitigate reputational damage.

The repeated breaches have placed Flagstar Bank under intense scrutiny, reinforcing the need for proactive and robust cybersecurity measures within the banking sector.