September 2017

Financial crimes observer

A publication of PwC's Financial Crimes Unit

Cyber and fraud: How to mitigate and prevent the next data breach

On September 7, Equifax, one of the three major credit agencies, publicly announced that it had suffered a major data breach. The company disclosed that unidentified hackers exploited a vulnerability in their website software to gain unauthorized access to company data and exfiltrated it from May through July of this year, impacting as many as 143 million consumers.[1]

The details of the attack — including the identity and nature of the attackers — are still developing.[2] If the attackers were financially motivated, they could monetize the data by fraudulently opening new accounts at financial institutions, conducting unauthorized transactions, and selling the data to other criminals. If a nation-state conducted the attack, the stolen information could be used to support espionage operations.

This data breach is the latest in a series of high-profile cybersecurity incidents, and is yet another reminder that organizations should enhance and better coordinate their cybersecurity and anti-fraud controls, including those related to identity management, authentication, data encryption, and patching vulnerable applications. Following such an attack, organizations should consider taking steps to identify customer accounts that may have been compromised and communicate with such customers what steps the organization is taking and what customers should be doing in response. Further, by conducting holistic risk assessments, developing a unified authentication strategy, and centralizing governance, organizations gain a better view of the threat landscape, better prevent and detect suspicious transactions, and streamline investigations.

This **Financial crimes observer** analyzes the risks associated with the data breach and provides our perspective on what organizations should be doing now.

pwc

What are the immediate risks?

The motives of the attackers — either financially motivated attackers or nation-state actors — will determine how stolen PII could be used.

Financially motivated attackers

If the attackers were financially motivated, they could use the stolen data to fraudulently open new accounts and gain access to existing ones.[3] Once in possession of personally identifiable information (PII) such as social security numbers, driver's license numbers, and full names, the attackers may attempt to order new credit cards, request new checkbooks, and open new accounts at financial institutions. They may also seek to modify existing account information and gain access to additional PII. PII presents greater risks than details gained from stolen credit card information because while credit cards can be voided, PII is intimately linked to particular individuals and can be used for a wider variety of fraudulent purposes such as those listed below:

- **Defeating existing identity verifications.** Attackers can use PII to answer account verification questions (such as "at which address have you previously resided?") that organizations ask before helping customers with any transactions, which include approving large transactions, home loans, new lines of credit, and new credit cards.
- **Creating and registering fraudulent accounts.** PII can be used to create fraudulent accounts from legitimate identities or synthetic identities.[4] In some cases, criminals create accounts where the legitimate user has never registered (e.g., Health Savings Account), making fraud prevention more difficult.
- **Changing passwords for online accounts.** PII provides data for criminals to guess password reset questions for online accounts. While most financial institutions have moved away from using this information as a form of online identification verification, several non-financial services firms (e.g., email providers, insurance, and retail services) still rely on this information for identity verification.
- **Selling stolen information to other criminals.** The attackers can sell stolen PII in online marketplaces to other criminals, who in turn can use the information to carry out the activities listed above.

Nation-state actors

If the attackers were nation-state cyber actors, the stolen data could be used for the following purposes:

- **Building intelligence dossiers on individuals and organizations.** Foreign intelligence services use PII to build dossiers on persons of interest for recruitment. While this type of activity would have a much less severe impact to the general consumer, it can significantly impact the national security of the US government, as it enables a foreign intelligence service to more clearly identify individuals and vet identity information of US persons. For example, foreign intelligence services responsible for data breaches at the Office of Personnel Management (OPM) used the compromised data to support espionage, counterintelligence, and competitive intelligence efforts.
- **Conducting espionage.** Foreign intelligence services may also attempt to gain access to key individuals' online accounts for espionage and counterintelligence purposes. An example of this would be Google's November 2016 warning to prominent journalists and academics (who may possess more relevant information) that government-backed attackers may have attempted to steal passwords.

What should organizations be doing now?

In the immediate aftermath of a data breach, organizations should take steps to identify the population of their at-risk clients and communicate with such clients regarding whether they were impacted and what they should do now. Compliance departments should closely follow federal and state regulations that may require that they inform customers or regulators within a prescribed time period.

Identify at-risk clients

Identifying impacted clients is no easy task, and the method to do so will vary by product. While all organizations should have methods in place to determine potentially compromised accounts (e.g., using behavioral analytics), financial institutions should take note of a few key considerations for various products. For credit cards, financial institutions should share with compromised parties (e.g., credit bureaus) the first 6 digits of credit card numbers (i.e, BIN ranges)[5] to help identify which client accounts have been compromised.[6] For lending products, the task is even more complex due to the potential number of parties involved (e.g., underwriters, loan originator, loan servicer, car dealerships, retailers). As a result, financial institutions will need to coordinate with these parties to identify which loans may have been exposed to the breach. Finally, financial institutions should remain aware that requests to open non-credit products such as checking accounts, trading accounts, and insurance products still result in a "soft ping" to credit bureaus; accordingly, customer PII for these accounts are also at risk.

Communicate with clients

Organizations should consider taking steps to communicate with their clients about the breach, and convey what is being done to mitigate potential exposure in the fastest and most effective manner. Once organizations have identified potentially impacted customers, they should suggest that such customers (1) perform a "credit freeze" to restrict a lender's access to the customer's credit report, (2) change password reset questions for online accounts to questions that do not rely on data that could be found in credit reports, and (3) stay alert regarding online scams using this data breach to solicit sensitive information, such as emails purporting to be from compromised parties that ask for sensitive data.[7]

After a breach, organizations will often receive a significant increase in call volumes from concerned customers. To manage this increased volume, organizations should put into place multi-channel outreach communication campaigns, including creating bespoke web pages to keep clients informed of developments and provide tips and helpful resources, in the hopes of diverting some inquiries away from the call centers.

Enhance cybersecurity and fraud controls

In addition to client identification and communication, organizations should consider taking the following steps (many of which are more long-term) to mitigate the risk from potentially exposed data and to reduce the probability of this type of event occurring in the future:

Cybersecurity controls

- Encrypt all sensitive personal customer data, including data "at rest."[8] This way, if an attacker does gain access, any sensitive data cannot be easily accessed and exploited.
- Harden and reduce your organization's attack surface by patching or moving vulnerable web applications behind firewalls or restricting access to these applications from external sources. Recent examples of this type of attack include the Apache Struts 2 vulnerabilities (CVE-2017-9805 and CVE-2017-5638).[9]
- Enhance identity proofing process and capabilities. Examples include having help desk staff call back clients at pre-registered phone numbers, requiring the use of Virtual Private Networks (VPNs) for remote access, and implementing account lockouts after a set number of failed logins.
- Use behavioral analytics to monitor and detect anomalous activity associated with users accessing sensitive data (e.g., user registration, help desk inquiries, password resets, sensitive business transactions).[10] By establishing normal network behavior by roles and job functions for accounts with access to sensitive information or systems, behavioral analytics can detect unknown malicious activity targeting an organization's critical assets.
- Stay abreast of government regulations mandating businesses to better protect customer data against identity theft.[11]

Anti-fraud controls

- Enhance authentication controls and policies, including requiring multi-factor authentication, biometric authentication (e.g., fingerprint scanning), or out-of-band authentication (i.e., verification through an additional channel such as text messages or telephone call backs).[12]
- Bolster controls related to account takeover, including developing or enhancing downstream controls to curtail the addition of an authorized user, updated physical address, and requests for additional credit or debit cards.
- Implement fraud analytics to develop or augment intelligence and analytical capabilities related to multiple new account applications - for example, those submitted with a single IP address or device ID.
- Provide guidance to call center staff to take extra steps when verifying customer identities to account for criminals employing social engineering techniques who may be posing as clients asking for password resets or other account management activities.
- Fortify the onboarding process for new merchant and business accounts and reinforce account update procedures for existing merchant and business accounts.
- Ensure that the organization does not rely on the type of stolen information for identity provisioning or identity and password reset services.
- Implement an internal communication plan to discuss potential impact to the business and next steps. This should include developing action plans, control changes, and metrics on the performance of mitigating controls, as well as conducting regular calls with senior leadership.

Integrate cybersecurity and fraud programs

Organizations should view the increase in number and severity of breaches as a wake up call to integrate elements of their cybersecurity and fraud programs. Doing so will provide a clearer view of the threat

landscape and a more coordinated process for investigations and reporting, which may help to prevent this type of attack in the future.

Accordingly, organizations can perform the following steps to more closely integrate their cyber and fraud programs:

- Pool data from cybersecurity and fraud departments into a central data repository. Using this data, identify red flags that could indicate suspicious transactions. Given the volume of transactions many organizations will need to analyze, we recommend using data analytics to identify suspicious signals (e.g., multiple failed login attempts, suspicious IP addresses) in a sea of transaction noise.
- Conduct holistic financial crime risk assessments, which should:
  - Evaluate and prioritize threats based on historic, known, and emerging trends in financial crime, including the Equifax attack.
  - Estimate the severity and likelihood of attacks, and inventory existing mitigating factors.
  - Assess risks based on the existence of current financial crime (cyber, fraud, anti-money laundering) controls, and recommend adjustments to controls and processes.
- Implement a cohesive case management system (i.e., a central repository for financial crime cases). Currently, many organizations have several case management systems for various areas of financial crime (e.g., cyber, fraud, anti-money laundering). With multiple systems used to capture data, investigators often fail to realize that cases they are working on have linkages to existing investigations and other areas of financial crime. Organizations that take a holistic approach to case management can respond more quickly to attacks, better prioritize investigations, and more efficiently distribute investigation workload.
- Enhance Suspicious Activity Report tracking and reporting processes to report the impact of the breach across the enterprise.
- Develop a coordinated process between cybersecurity and fraud teams for incident response and crisis management processes and procedures. This includes providing a central governance process for investigations, which should include clearly defined escalation paths and communication plans.

Endnotes

1. Equifax handles sensitive data — including full names, social security numbers, birth dates, and home addresses — for 820 million consumers and 91 million businesses. In addition, US consumers' driver's license numbers, credit card information, dispute documents used to challenge credit ratings, as well as other undisclosed personal information on UK and Canadian residents were also potentially exposed. For additional information, see the New York Times, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.* (September 2017).
2. The Apache Software Foundation, in a September 9 *online statement,* acknowledged press reports that the Equifax breach was "potentially carried out by exploiting a vulnerability in the Apache Struts Web Framework." The statement said that this remained unconfirmed and it was unclear which Struts vulnerability, if any, would have been utilized to execute the breach. For additional information, see *The Next Cyber Threat Is Here: What You Need To Know* (September 2017).
3. For additional information on account takeover, see PwC's *Financial crimes observer, Fraud: Email compromise on the rise* (February 2016).
4. A synthetic identity is the creation of a fake individual using bits of PII from different, real individuals (e.g, one individual's postal address, another person's phone number). Because most firms only check these details in isolation from each other, attackers can potentially use synthetic identities to open fraudulent accounts.
5. BIN ranges of credit cards identify the issuing bank and the network the card belong to, while the other numbers are generated randomly.
6. Credit card providers should share these BIN ranges with credit reporting agencies because such agencies have direct relationships with credit card providers, and while they can't divulge information due to Fair Credit Reporting Act requirements, they can confirm whether specific bank clients have been impacted.
7. These fraudulent emails could be sent from official accounts that have been compromised, making it difficult to determine their validity. For additional information, see the *Financial crimes observer* cited in note 3.
8. Data "at-rest" refers to data that is not actively moving, such as data stored on a hard drive or server. For additional information on data encryption, see PwC's *Financial crimes observer, Cyber: New York regulator moves the goalposts* (September 2016).
9. For additional information on the Apache Struts vulnerabilities, see note 2.
10. For additional information on behavioral analytics, see PwC's *Financial crimes observer, Fraud: Old defenses won't stop new threats (*April 2016).
11. Examples of such regulations include a proposal released by the Federal Reserve Board, Office of the Comptroller of the Currency, and the Federal Deposit Insurance Commission last year, and a final rule released earlier this year by the New York Department of Financial Services. For additional information, see PwC's *Financial crimes observer, Cyber: Banking regulators weigh in* (November 2016) and the *Financial crimes observer* cited in note 1.
12. For additional information on multi-factor authentication and other enhanced authentication techniques, see the *Financial crimes observer* cited in note 6.

Additional information

For additional information about this **Financial crimes observer** or PwC's Financial Crimes Unit, please contact:

Julien Courbe
Financial Services Advisory Leader
646 471 4771
julien.courbe@pwc.com
@JulienCourbe

Sean Joyce
Financial Crimes Unit Leader
703 918 3528
sean.joyce@pwc.com
@RealSeanJoyce

Jeff Lavine
Financial Crimes Unit Chief Operating Officer
703 918 1379
jeff.lavine@us.pwc.com

Joseph Nocera
Cybersecurity Leader
312 298 2745
joseph.nocera@pwc.com
@JoeNocera_PwC

Brian Castelli
Anti-Fraud Leader
646 471 2563
brian.castelli@pwc.com

Genevieve Gimbert
Anti-Fraud Leader
646 471 5145
genevieve.d.gimbert@pwc.com
@GenGimbert

John Sabatini
AML and Sanctions Leader
646 471 0335
john.a.sabatini@pwc.com

Roberto Rodriguez
Director of Regulatory Strategy
646 471 2604
roberto.j.rodriguez@pwc.com

Contributing authors: Haris Shawl, Adam Malone, David Fapohunda, Astrid Yee-Sobraques, Michael Compton, Christopher Castelli, and Michael Horn.

Follow us on Twitter @PwC_US_FinSrvcs