EXPOSED CREDENTIALS MONITORING_

SOLUTIONS GUIDE & BEST PRACTICES FOR RESPONSE

digital shadows_

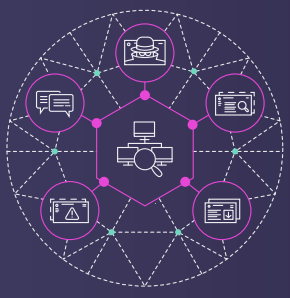
PREVENTING ACCESS TO SENSITIVE DATA

Exposed credentials are email address and password pairs found on the open, deep, or dark web. The credentials are often found within a data leak that has been made public or advertised for sale in marketplaces or forums. Alternatively, they are exposed through accidental release of configuration files containing sensitive data.

The credentials may be leaked from a corporate system, a service provider, or a third party system used personally by employees. It is common for employees to use work email addresses for personal reasons as well as corporate system access.

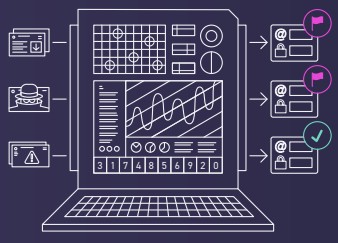
According to Google, more than 50% of people are suspected to reuse passwords. If these exposed credentials are valid, they have the potential to provide access to corporate systems, cloud services or other third parties.

This guide draws from best practices suggested in SearchLight's playbooks, so security professionals can improve their tools and processes to prevent employee account takeover.



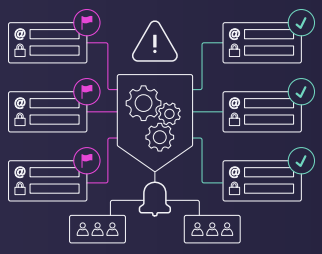
COLLECT

COLLECT FROM OPEN, DEEP, AND DARK WEB SOURCES



VALIDATE

ASSESS VALIDITY OF CREDENTIAL AND SOURCE CONTEXT



CONTAIN

RESET AFFECTED CREDENTIALS AND INFORM USER

EDUCATE

REFINE POLICES AND EDUCATE EMPLOYEES

COLLECT

The value of breached credentials to cybercriminals changes over time. When credentials are newly breached, they are often shared privately between individuals for high prices. Gradually, these breaches are shared more widely and for lower values. Eventually, these credentials become ubiquitously shared across criminal forums and paste sites for free.

Organizations that can detect their employees' credentials within these breaches as early as possible stand the best chance of preventing access to valid employee accounts. The most common sources of exposed credentials are criminal forums, dark web marketplaces, Telegram Channels, IRC channels, code repositories, and paste sites.

The first challenge for security practitioners is to keep up-to-date with new breaches and the numbers are significant. Since July 1 2020, Digital Shadows has detected 5 billion exposed credential pairs across more than 700 breaches. This brings the total number of breached credentials in circulation to over 20 billion.

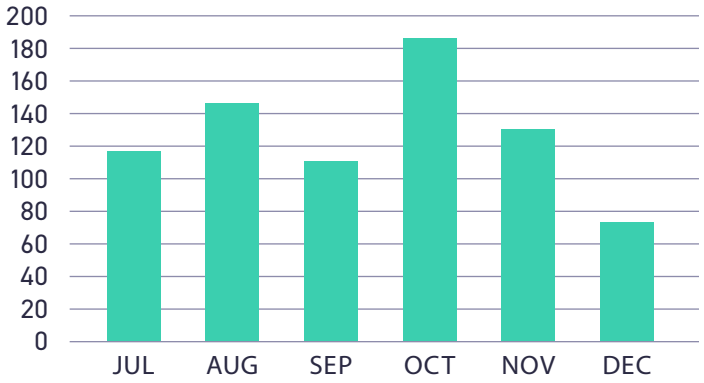
The second challenge is to store all of this data, which can be a daunting task. Troy Hunt, the founder of HaveIBeenPwned explained his challenges storing hundreds of millions of credentials, and the journey from storing data in SQL Server to Azure Table Storage.

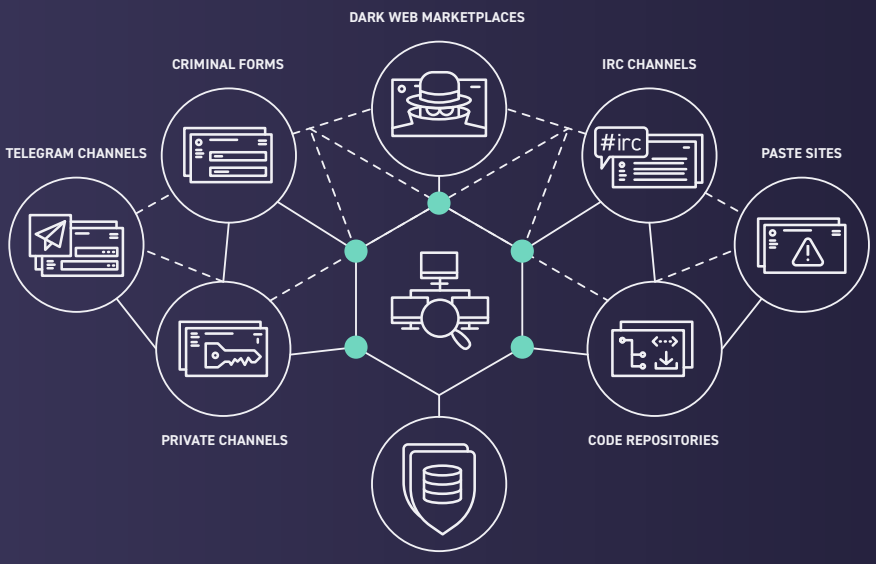
SINCE JULY 1 2020
DIGITAL SHADOWS DETECTED

5 BILLION

EXPOSED CREDENTIAL PAIRS
ACROSS 700 BREACHES

NUMBER OF BREACHES INGESTED BY DIGITAL SHADOWS IN H2 2020





VALIDATE

NIST RESPONSE STAGE: DETECTION & ANALYSIS
SANS INCIDENT RESPONSE: IDENTIFICATION

As a security precaution, some organizations may choose to reset accounts even if no password has been exposed. However, given the number of breaches reported each month, this approach can quickly snowball, create unnecessary friction for users, and ultimately lead to password fatigue.

There is no way to identify the age or validity of credentials from the credential itself. Many "new" data leaks include credentials from previous leaks, sometimes from a long time ago. This recycling of credentials increases the perceived volume of credentials circulating.

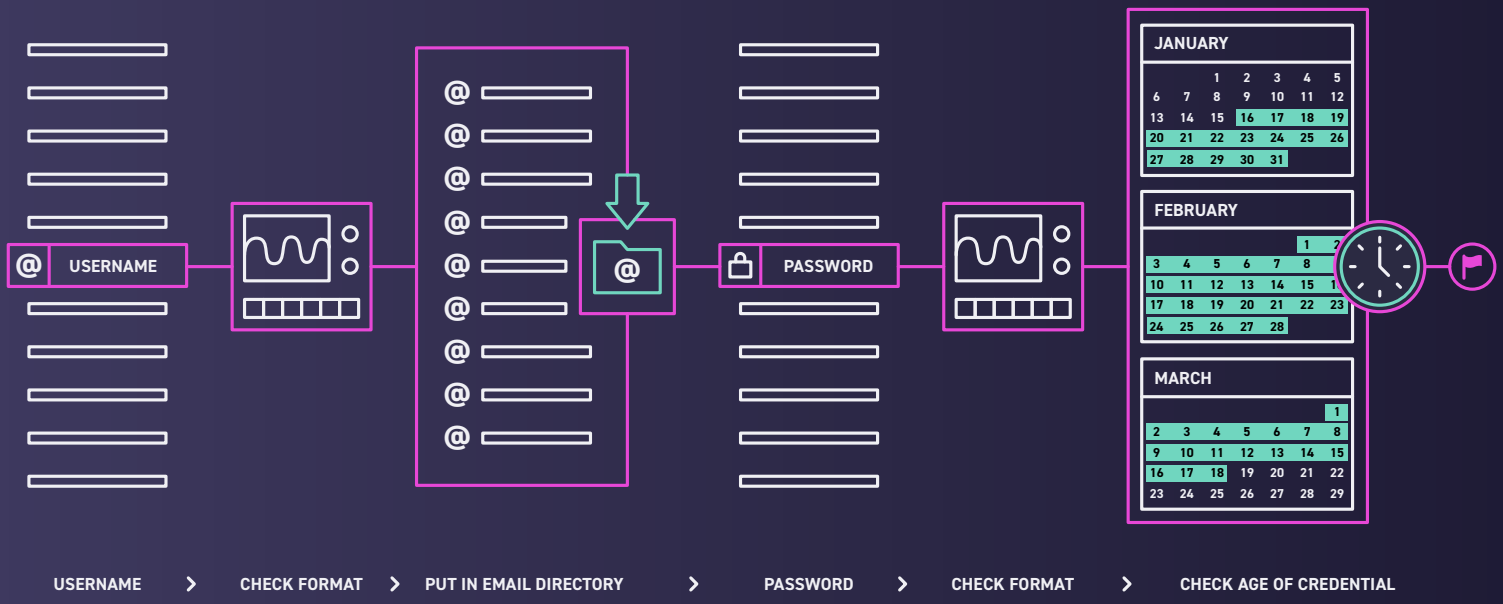
Security teams are often focused on one core question: are any of these breached passwords authentic and provide access to my company's systems today?

For example, the user account may have been deactivated, the password may not meet the password requirements for internal systems, or it is so old that the credential pair is no longer valid. This is not always straightforward, as departmental email addresses (i.e. accounts@acme.com) do not always follow the same formats as individual email addresses.

Credentials investigation is often the most time-consuming stage for security teams, who spend hours in the week trying to understand if the exposed credentials represent a valid threat to the company.

For this reason, we recommend starting only with breached credentials that contain both an email AND a password, which makes it easier to ascertain if it can provide genuine access.

You can read more about Digital Shadows' credential validation methods here.



CONTAIN

NIST RESPONSE STAGE: CONTAINMENT, ERADICATION & RECOVERY
SANS INCIDENCE RESPONSE: CONTAINMENT, ERADICATION

Once a password pair has been validated, speed to alert the users to reset their passwords becomes key.

Not all accounts are equal: C-Level and accounting personnel should be addressed with higher priority. A staggering 33,000 of exposed credentials are for accounting inboxes.

More mature organizations that store their own breached passwords may choose to impose further restrictions on their users' new password selections. This involves assessing new passwords against the growing list of breached passwords, and prompting the user to pick another password.

RESET CREDENTIAL

If the credential is valid for a corporate system, reset passwords for the associate user. Admin and VIP credential resets may require more support.

CONDUCT DEEPER ANALYSIS

Search logs to identify unusual usage by an affected user. Set up alerts in SIEM systems for unexpected behavior like logging in to admin systems, going to new suspicious domains, or moving large amounts of data out of corporate systems.

COMMUNICATE INCIDENT TO AFFECTED USERS

Notify users that they have had a credential exposed and guide them to reset any services using this password. Providing the leaked password as context can motivate users to act more promptly.

EDUCATE

SANS INCIDENT RESPONSE: LESSONS LEARNED

Once the initial fire has been put out and the valid account has been reset, there is a chance to step back and understand what lessons can be learned.

First, the user may still be at risk if they are reusing passwords across multiple other accounts. Therefore, educating the user of responsible password usage is critical.

More mature organizations will use this type of data to tailor their training. Some security teams will prevent users from using passwords that are the most commonly used. Check out NordPass' list of the most common passwords of 2020 for further information.

37.9%

THE AVERAGE CLICK-THROUGH RATE IN 2020 ACCORDING TO KNOWBE4

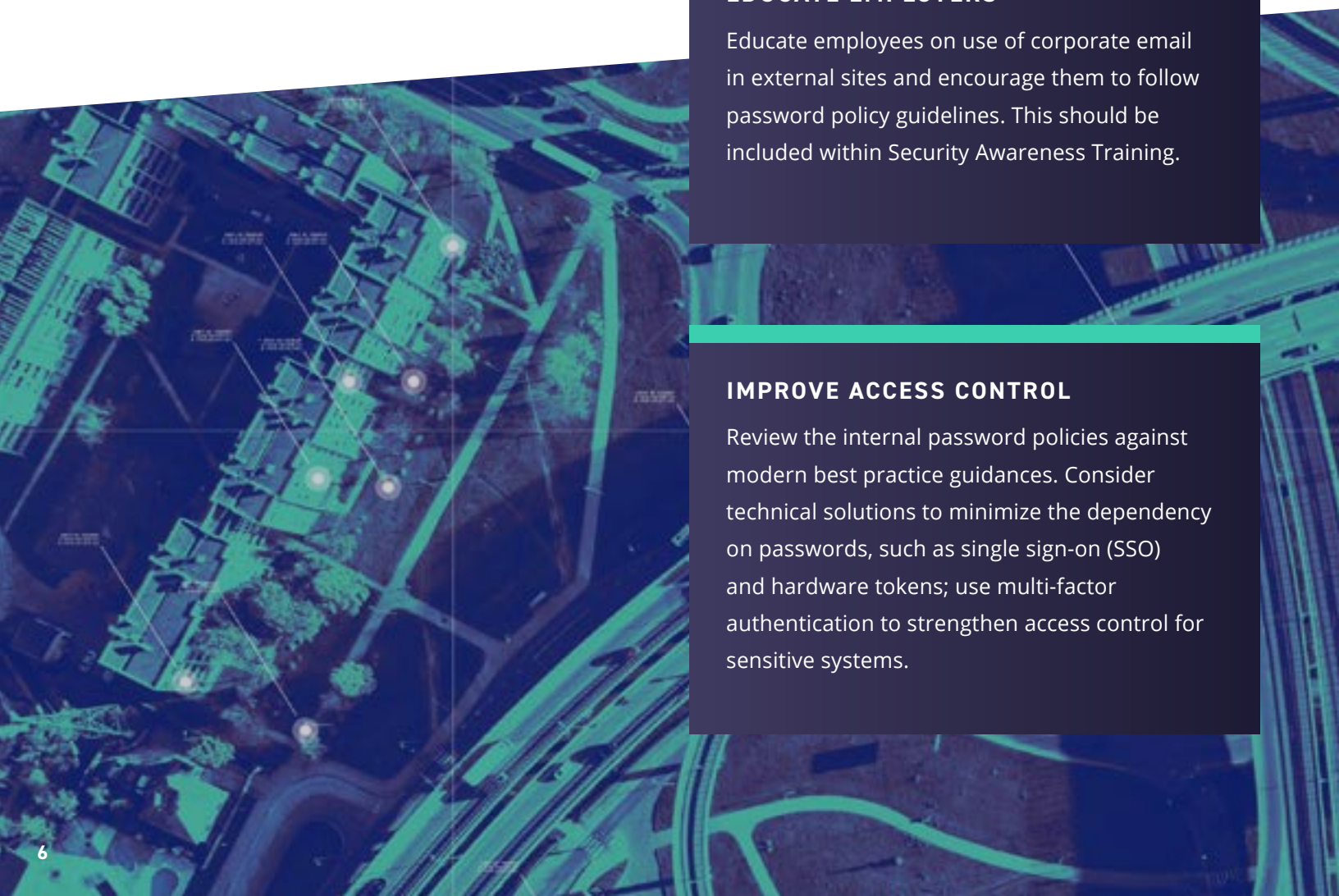
www.knowbe4.com/hubfs/2020_PhishingByIndustryBenchmarkingReport.pdf

EDUCATE EMPLOYERS

Educate employees on use of corporate email in external sites and encourage them to follow password policy guidelines. This should be included within Security Awareness Training.

IMPROVE ACCESS CONTROL

Review the internal password policies against modern best practice guidances. Consider technical solutions to minimize the dependency on passwords, such as single sign-on (SSO) and hardware tokens; use multi-factor authentication to strengthen access control for sensitive systems.



MITIGATION & RESOURCES

Successful exposed credential monitoring can be one of the most actionable types of threat intelligence. We've pulled together a list of resources that will help organizations to begin or enhance their maturity for detecting exposed employee emails and passwords.

Implement multi-factor authentication that doesn't use SMS messages. This can help reduce ATO, but should be balanced against the friction (and cost) it can cause. The Photon Research team's report Two-Factor In Review: A technical assessment of the most popular mitigation for account takeover attacks details the technologies involved with 2FA, attacks against the solution, and ways to mitigate.

Subscribe to a credential monitoring service for free. Monitor for leaked credentials of your employees. HaveIBeenPwned is a great resource for this, alerting you to instances of breaches and including your organization's email domain. Although HaveIBeenPwned doesn't provide you with passwords, it's a great place to start identifying which accounts are potentially compromised.

You can also sign up for a Test Drive of SearchLight to search across paste sites and criminal forums.

Monitor code repositories. Code repositories can be rich with secrets and hard-coded passwords, but there are some great (free and open-source) tools, such as TruffleHog and GitRob, that comb them for access keys, authentication tokens, and client secrets.

Increase user awareness. Educate your staff and consumers about the dangers of using corporate email addresses for personal accounts, as well as reusing passwords.

Maintain awareness of credential stuffing tools. Keep an eye on the development of OpenBullet and others, and monitor how your security solutions are protecting against evolving capabilities (such as bypassing CAPTCHA).

Deploy an inline Web Application Firewall. Commercial and open-source web application firewalls, like ModSecurity, can identify and block credential stuffing attacks.

Monitor for references to your company and brand names on cracking forums. Configuration files for your website that are being actively shared and downloaded are a good indication of impending ATO attempts. Use Google Alerts for this monitoring, which identifies the risks specific to your business; check out the Google Hacking Database for some great tips.

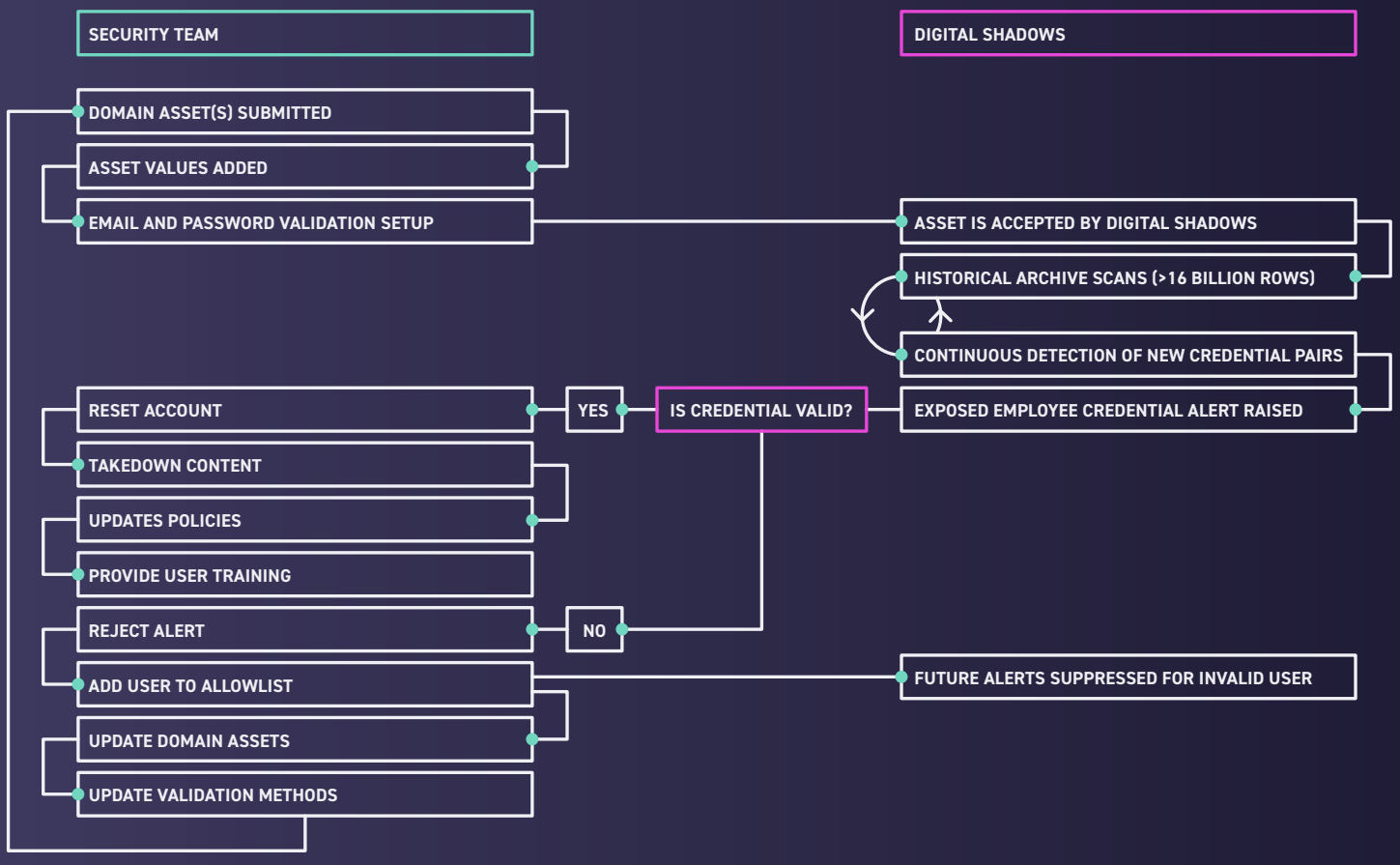
THE DIGITAL SHADOWS WORKFLOW

Digital Shadows SearchLight™ helps organizations with exposed credential monitoring, continually scanning and adding to a repository of more than 20 billion credentials.

This includes multiple methods of credential validation, including integrations with Okta and Azure Active Directory, as well as the ability to specify email/password format and upload an email list to validate against. Users can go further by automatically discarding credentials that do not pass the validation.

SearchLight also saves time by enabling users to add credential pairs to an allowlist, which will prevent exposed passwords of expired accounts from having to be triaged again.

Integrations with Splunk Phantom and XSOAR help to add further elements of remediation.



THANK YOU_

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threat. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface.

To learn more and get free access to SearchLight™, visit
www.digitalshadows.com

London
Columbus Building, Level 6,
7 Westferry Circus,
London, E14 4HD
+44 (0) 203 393 7001

San Francisco
235 Pine St. Suite 1050,
San Francisco, CA 94104
+1 (888) 889 4143

Dallas
5307 E. Mockingbird Ln.
Suite 200
Dallas, TX 75206