

Security Awareness Training Partner Guide

Dark Web Monitoring Notification Setup & Overview

Internal Use Only



#HACKERS SUCK

www.TrustTelesystem.com

Dark Web Monitoring Partner Guide

Table of Contents

Dark Web Monitoring Overview <i>getting started & feature overview</i>	page 3
Purchasing Dark Web Licenses <i>for clients in unlimited training product</i>	pages 4 – 5
Configuring Dark Web Notifications <i>notification configuration & initiation</i>	pages 6 - 7
Dark Web Reports and Notifications <i>view dark web results</i>	pages 8 – 9

Dark Web Monitoring Overview

Create ongoing value for your clients with Dark Web Monitoring. Receive automated alerts if/when your client's email domain is found on the Dark Web to provide immediate remediation.

Getting Started

Why Dark Web Monitoring?

Dark Web Monitoring is an essential addition to every Managed Services offering, another addition to the state of security to monitor and protect your clients.

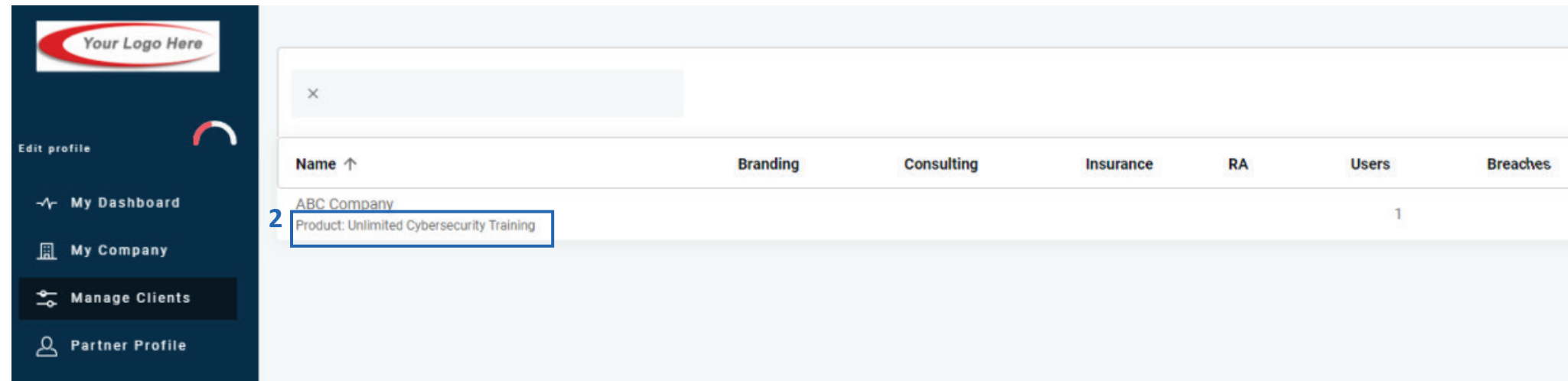
How does it Work?

1. All Breach Prevention Platform (BPP), HIPAA BPP, EVA MD and Partner HIPAA Compliance clients receive Dark Web Monitoring for up to 3 domains
2. Dark Web Monitoring can be purchased as an add-on to the Partner Subscription in blocks of 10 domains for Unlimited Training clients who request monitoring.

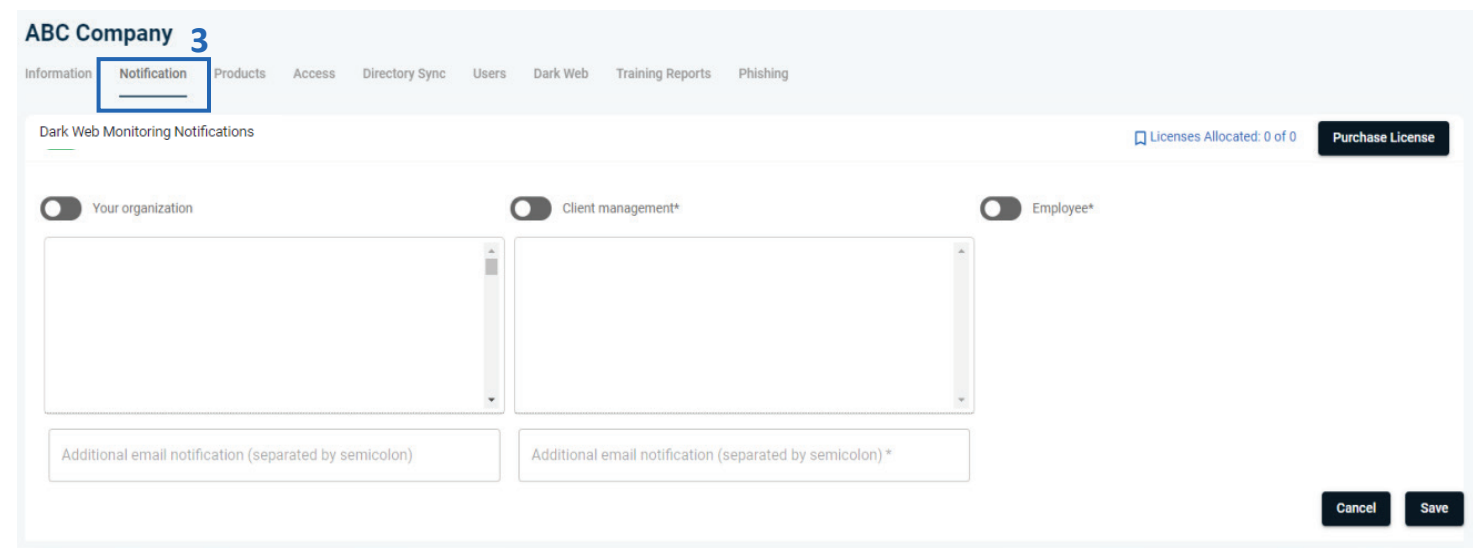
Purchasing Dark Web Licenses

Dark Web Monitoring services are included for clients in the BPP, HIPAA BPP and EVA MD products and do not require purchase of additional licenses. For clients in the Unlimited Training product, Dark Web Monitoring blocks can be purchased and applied to enable this continuous monitoring feature.

Purchasing Licenses



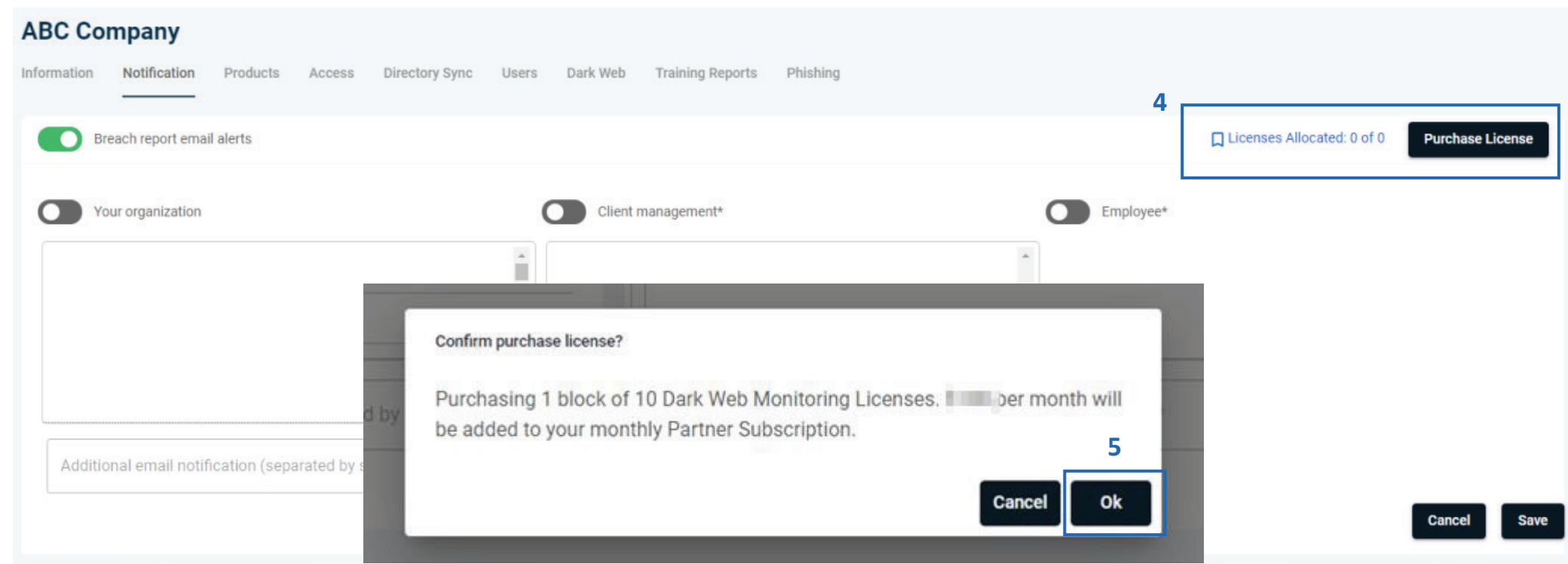
1. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in, select “**Manage Clients**” to access your client list (above).
2. Select a client in the Unlimited Cybersecurity Training product you would like to enable Dark Web Monitoring notifications for.
3. Select the “**Notification**” tab, then select Dark Web Monitoring Notifications



Purchasing Dark Web Licenses

Dark Web Monitoring services are included for clients in the BPP, HIPAA BPP and EVA MD products and do not require purchase of additional licenses. For clients in the Unlimited Training product, Dark Web Monitoring blocks can be purchased and applied to enable this continuous monitoring feature.

Purchasing Licenses



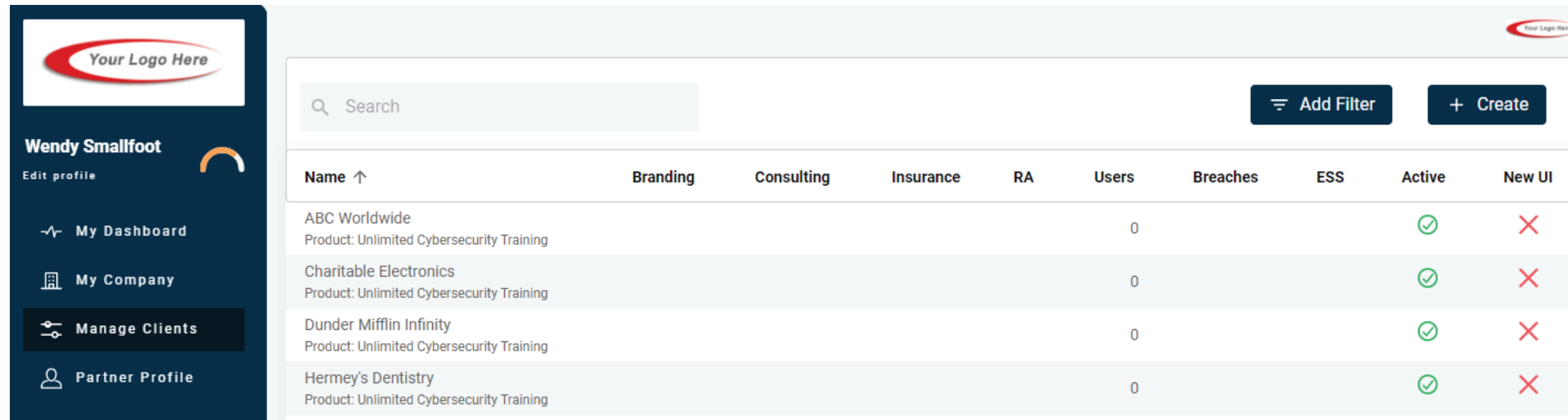
4. If you do not have any licenses and wish to configure Dark Web Monitoring for clients in the Unlimited Cybersecurity Training product, click the “Purchase Licenses” button at the top right of the screen. Confirm your purchase on the pop-up window to add 1 block of 10 domains for \$110 per month.
5. Confirm your purchase on the pop-up window to add 1 block of 10 domains for \$110 per month.

You can now allocate licenses for existing or new Unlimited Training clients. To allocate licenses, continue to the [Configuring Dark Web Notifications](#) section.

Configuring Dark Web Notifications

Learn how to enable and configure Dark Web Monitoring notifications for your clients! Clients in the BPP, HIPAA BPP, EVA MD and Partner HIPAA Compliance product receive monitoring for up to 3 domains. Unlimited Training clients can receive monitoring with the purchase of DWM licenses.

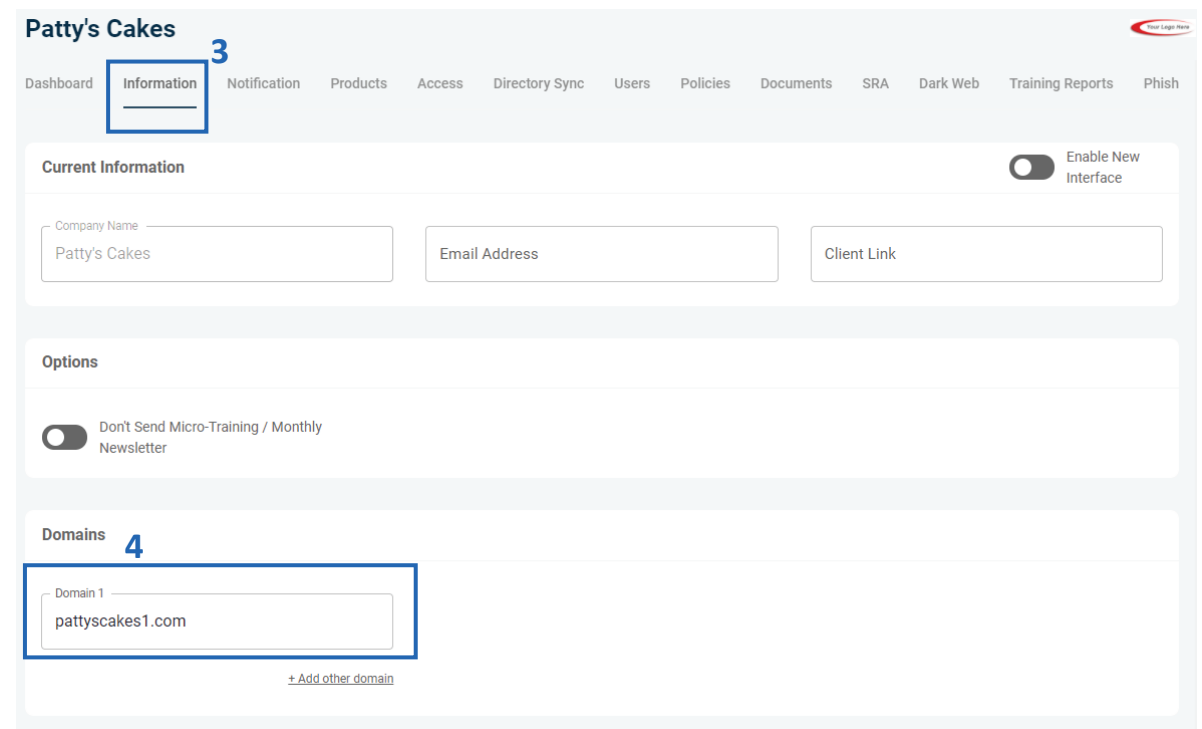
Navigating to the Dark Web Monitoring



The screenshot shows the PII-Protect portal interface. On the left is a dark sidebar with the user's name 'Wendy Smallfoot' and a 'Manage Clients' button. The main area displays a table of clients with columns for Name, Branding, Consulting, Insurance, RA, Users, Breaches, ESS, Active, and New UI. The table lists four clients: ABC Worldwide, Charitable Electronics, Dunder Mifflin Infinity, and Hermey's Dentistry, all with 0 breaches and active status.

Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			✓	✗

1. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in, select “**Manage Clients**” to access your client list (above).
2. Select the client you would like to enable Dark Web Monitoring notifications for.
3. Select the “**Information**” tab
4. In the “**Domains**” section, add the client’s domain(s) you are looking to monitor, if not already done.
5. Click the “**Save**” button at the bottom of the page.



The screenshot shows the configuration page for 'Patty's Cakes'. The 'Information' tab is selected. The 'Current Information' section includes fields for Company Name (Patty's Cakes), Email Address, and Client Link. The 'Options' section has a toggle for 'Don't Send Micro-Training / Monthly Newsletter'. The 'Domains' section shows a list of domains with 'pattyscakes1.com' entered in the 'Domain 1' field. A blue box highlights the 'Information' tab and the 'Domains' section, with a blue '3' next to the tab and a blue '4' next to the 'Domains' section header.

Configuring Dark Web Notifications

Learn how to enable and configure Dark Web Monitoring notifications for your clients! Clients in the BPP, HIPAA BPP, EVA MD and Partner HIPAA Compliance product receive monitoring for up to 3 domains. Unlimited Training clients can receive monitoring with the purchase of DWM licenses.

Dark Web Alert Configurations

6. Within the same client, navigate to the “**Notification**” tab, then open Dark Web Monitoring Notifications.

7. Use the slider to turn “**Breach Report Email Alerts**” on.

8. Select who you want to receive an email alert in the event of a data breach.

- Your Organization – anyone listed as a Partner Administrator under your partner account, a distribution list, or ticketing system.
- Client Management – anyone listed as a manager under that client
- Employee – notification will be sent to the email address involved in the data breach
- Under “Additional Email Notification”, you can add email addresses that are not in the portal

9. Click “**Save**” to save your selections. These selections can be changed/updated at any later point

Viewing Dark Web Reports

When domain(s) are entered for a client, a Dark Web Report is available with the results from the scanned domain(s). These results can be shared with clients in report format to create actionable remediation steps.

Navigating to Dark Web results

The screenshot shows the 'Dark Web' tab selected in the top navigation bar. A table lists various breaches with columns for Account, Site Breached, Breach Date, Confidence Score, and Password. A popup window provides details for the 'NetProspex' breach, including the actor's name and a description of the breach.

Account	Site Breached	Breach Date	Confidence Score	Password
ashleymadison.com	36M			XXXXXXXXXXXXX...
NetProspex				Passwords Compromised
LinkedIn				Passwords Compromised
clearvoicesurveys.com	13.4M	2021-04-23	100	xhXXXXXXkf
clearvoicesurveys.com	13.4M	2021-04-23	100	xhXXXXXXkf

NetProspex Breach Details:

- Actor:** Yevgeniy Nikulin
- Description:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

1. Click on the client you are wishing to view the Dark Web results for.
2. Select the “**Dark Web**” tab at the top of the page.
3. The results from the scanned domain(s) are found on this page with details on the account compromised, site breached, date of breach, Confidence Score and the exposed password.
4. A Dark Web report can be generated by clicking the “Generate Reports” button. Two reports will be sent to your email address; one will be a Summary Report PDF with details on the breaches and action items for clients, along with a Summary Report excel file with all breach details in a formattable document.
5. You can search for a specific user or breach with the “Search” feature.
6. Clicking the “down arrow” will show details of additional compromised data.
7. A description of the breach (if available) is shown by clicking on the “information icon” next to the site breached.

Sample Dark Web Notifications

When breaches affecting your client's domain(s) are discovered on the Dark Web, notifications are promptly sent out based on your configurations.

Sample of Partner Breach Notification Email

6. If a user's email was found on the Dark Web an email notification will be sent based on the configurations set in the portal.
7. A sample Dark Web Breach Notification sent to a Partner is provided.
8. Note: Client Management and Employee Breach Notification emails will be similar.

DARK WEB BREACH NOTIFICATION

Hi [REDACTED]

Thanks to a diligent cybersecurity program, your personal Dark Web security guard has found some suspicious activity.

Company: [REDACTED]

[ACCOUNT LOGIN](#)

Through continuous monitoring of the Dark Web, we have found that your client, [REDACTED] had 2 employees whose email addresses were recently involved in a data breach. Please see the table below for further information regarding this incident.

Account	Breach	Confidence Score
[REDACTED]	COMB - Compilation of Many Breaches, Part 43	40
[REDACTED]	COMB - Compilation of Many Breaches, Part 1	40

We know data breaches are alarming for not only you, but for your clients as well, so we recommend following up with all parties involved, as well as logging into the portal to view further details. If you have any questions or concerns, please feel free to reach out to us.

Thank you,

[Account Login](#)



You're All Set!

_____ Don't forget to checkout our Breach Secure Now Service Breakdown to determine which of our per-client upgrades are best for your clients [here!](#)

 **Telesystem**[®]
IT's About Trust[®]

#HACKERS SUCK

www.TrustTelesystem.com