PVH CORP. ANTI-FRAUD INFORMATION GUIDE

PVH CALVIN KLEIN TOMMY HILFIGER HERITAGE BRANDS

Counterfeit Product

Unfortunately, there are many instances of counterfeit product of PVH brands, including *CALVIN KLEIN, TOMMY HILFIGER, Van Heusen, IZOD, ARROW, Speedo, Warner's, Olga, Geoffrey Beene* and *True&Co.*, both online and in physical stores/stalls. It can also be difficult to distinguish between genuine and counterfeit product, especially online.

If you find a retailer that may be offering counterfeit product of any PVH brand or you have concerns about the legitimacy of product that you purchased, please reach out to us and provide as many details as you can. You can send the information to enforcement@pvh or via our customer service channels. This will help us to identify the potential problem and follow up accordingly.

Please note that purchasing products from unauthorized retailers is always at your own risk. Please be careful.

Online Scams

Email scams (phishing) are increasingly common scams used by fraudsters to get personal information from people, usually in an attempt to take money out of a victim's bank account, use their credit cards or to open new credit accounts.

Email Scams (Phishing)

Phishing is the practice of sending phony email messages that are disguised as legitimate communications, often with company logos and consumer account information that looks real. In most cases, any email scam is based on messages sent to random email addresses, both PVH and non-PVH customers, and is not the result of any breach at PVH.

If you receive an email claiming to be from PVH or any of its brands that you believe may be fraudulent, **do not respond and do not click on any links or open attachments contained within the email**. If you accidentally clicked the link and entered your password, you should immediately change your password anywhere you used that username and password.

For more information on how to identify a potential email scam, see the *'How can I tell an email is Fraudulent'* in our FAQ.

Job Posting Scams

One type of scam involves the use of fake job postings. These scammers may advertise jobs alongside legitimate job postings online, in newspapers and on other media.

Online Scams (cont.)

All current job opportunities with PVH (including *CALVIN KLEIN* and *TOMMY HILFIGER*) are available here.

Warning signs that a job opportunity might be fraudulent include being asked to pay for a job placement, being asked for sensitive personal information over the phone, and being offered a job without meeting anyone from PVH or one of its brands. Additional red flags are discussed in the 'How can I tell that a job opportunity is fraudulent' section of our FAQ.

For more information on how to identify or report a fraudulent job scam, see our FAQ.

To Report a Suspicious Email or Potential Scam

Identifying and investigating potential scams is handled by law enforcement. We encourage anyone who believes that they have been targeted by a fraudster to contact the Anti-Phishing Working Group at reportphishing@apwg.org and to file a report with the Federal Trade Commission, the Federal Bureau of Investigation Internet Crime Complaint Unit, and/or the Department of Justice. If you are located outside of the United States, you should contact the appropriate government agency and/or your local law enforcement.

You can also notify PVH by forwarding the email or potential scam to reportfraud@pvh.com.

If you responded to a suspicious email, gave personal information or have lost money, please contact your local police department.

FAQ

Why am I constantly receiving fraudulent emails?

Scam artists may have obtained your email address from a variety of sources.

- They may have used a spam mailing list on which your email address was listed with or without your consent. These lists are sometimes created from online contest entries. Always be sure to check out the legitimacy of a company before you enter their online contest.
- They may have obtained your email address via spyware installed without your knowledge on your PC. Make sure your computer is protected against spyware.
- They may have created hundreds of thousands of email addresses randomly by combining first and last names and known domain names, one of which happens to be your personal email address.
- Your email address may have been included in an online breach of other retailers or internet websites that have no connection to PVH.

FAQ (cont.)

Once scam artists find an email address that works, they may send emails to that address repeatedly.
Though phishing is generally associated with email, some criminals use the phone as well. In this case, scam artists call victims on the phone and pose as a financial institution employee, an investigator or a police officer.

How can I tell if an email is fraudulent?

You must be extremely careful, because scam artists use the colors and logos of legitimate websites to make their phony emails look real.

To differentiate a phishing email from a legitimate one, pay specific attention to the content of the message, including any attachments or websites you are asked to click. Attackers will use logos, signatures, security elements and backgrounds that are identical to the originals. Most legitimate companies will not send you attachments. Instead of clicking links contained within an email, open your internet browser and type in the company's website directly.

If you receive an email you believe to be fraudulent, you may forward it to reportfraud@pvh.com for confirmation.

Can I protect myself against phishing attempts?

Unfortunately, you may occasionally receive fraudulent emails which appear to have been sent by PVH or other companies that you have used in the past.

Your best protection is to stay vigilant:

- Never respond to an email requesting personal information without confirming the source.
- Never open email attachments if you don't know the sender.
- Look for a closed padlock in your browser's status bar, ensuring you are in a secured online environment. Also make sure the address displayed has an "s" in "https". You should also be able to view the site's digital certificates by double-clicking on the little closed padlock in your browser's status bar.

Also ensure your personal computer is adequately protected with the necessary security software.

- Install all of your computer's recommended security updates.
- Install a version of anti-virus software that includes automatic updates.
- Backup your personal data on a regular basis
- Pick strong passwords and leverage two-factor logins when available.

FAQ (cont.)

How can I tell that the job opportunity is fraudulent?

Here are some warning signs that the job opportunity may be fraudulent:

- You are asked to pay for a job placement
- You are asked to transfer or wire funds between accounts
- You are sent a large check and its requested that you cash it in your personal account
- You are sent gift cards for the purchase of home office equipment
- You are asked for sensitive personal information like your social security number or bank account outside of the onboarding process
- The hiring manager offers you the position without talking or meeting with you
- The hiring manager uses a personal email address or an address that doesn't match the PVH name or any of its brands

What do I do if I was targeted by a fraudulent job scam?

If you feel you have been targeted by a job scam, you can file a report or complaint with the Federal Bureau of Investigation Internet Crime Complaint Unit, the U.S. Department of Justice, the Federal Trade Commission and/or your local police department. If you are located outside of the United States, you should contact the appropriate government agency and/or your local law enforcement.