AP / TIJANA MARTIN

Big-screen TVs will be a hit this holiday season, experts say.

THE ISSUE: SHOPPING

Be smart on Black Friday

BY SHERYL NANCE-NASH
Special to Newsday

There's shopping and then there's smart shopping. When it comes to Black Friday, if you don't get it right, you've missed opportunities that can be costly.

Some stuff you want to snap up, but other stuff is best put on your "buy later" list. The experts share insight.

■ **What to buy**: Michael Bonebright, a consumer analyst with DealNews.com, says big-screen TVs are going to be the best doorbusters. "Best Buy will have a huge Samsung 70-inch 4K Smart TV for just $550. That's the best price we've ever seen for any name-brand TV of this size. Target will offer an Element 65-inch 4K Roku TV for $280. Before this deal, the lowest price we'd seen for a Roku TV like this was $400."

Another big category we're seeing this year is smart home gadgets. "The Google Home Mini is going to be the cheapest smart speaker this year. Both Dell and Target will have the device for only $19 — that's $3 under what most stores are going to charge for the third-generation Amazon Echo Dot," Boneright says.

Expect deals on trendy electronics. "Over the last three years, the best discounts on products lik.e Beats by Dre headphones always happen on Black Friday weekend. The same goes for products like GoPro camera bundles," says Kristin Cook, editor in chief of Ben's Bargains.

■ **What to skip**: Wait to get those sneakers you've been eyeing. "Sneakers are cheaper on 66% of days throughout the year than they are on Black Friday," says Danny McLoughlin, content and research director for RunRepeat.com, which reviews athletic footwear.

Breach notice law's new obligations

SMALL BUSINESS
Jamie Herzlich
jherzlich@aol.com

Part of a state data breach notification law went into effect last month, and companies need to be aware of their new cybersecurity responsibilities and the penalties they could face if they don't protect customer information, experts say.

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act signed into law in July broadens the scope of information that could trigger a breach notification to consumers and requires businesses to adopt more stringent data security safeguards.

"It's a significant change for all businesses not only within New York State, but outside of New York that collect, process or otherwise control personal information of NY residents," says Jessica Rando-Copeland, a member in the Buffalo office of Bond, Schoeneck & King.

The breach notification updates became effective Oct. 23 and the data security requirements take effect March 21, 2020.

"I don't think people really get it yet," says Chris Zegers, director of consulting at Hauppauge-based Ivionics Legal, the legal operations management consulting arm of IT firm Ivionics.

New York State had breach notification requirements previously, but this law expands upon those requirements and for the first time sets standards and safeguards that businesses outside of regulated industries should take to protect residents' data, Rando-Copeland says.

SHIELD compliance aims to arm consumers with knowledge about breaches so that they can be more vigilant about monitoring their credit reports, credit scores, credit card activity and online banking transactions, Rando-Copeland said.

Among its provisions, the legislation expands the definition of what constitutes private information to include biometric information (i.e. fingerprints/retina image) and email addresses and corresponding passwords or security questions and answers, she says.

It also broadens the definition of a breach to include unauthorized access to private information, said Stephen Breidenbach, co-chair of the Cybersecurity, Privacy and Technology Practice at Moritt Hock & Hamroff LLP in Garden City. "One important note is that this is a consumer protection statute and, therefore, any ambiguity in the statute would likely be interpreted in favor of the consumer."

This is a step in the right direction considering cyberattacks are the fastest-growing crime in the United States, according to Northport-based Cybersecurity Ventures, a provider of data and analytics for the cybersecurity industry.

The firm predicts cybercrime will cost the world $6 trillion annually by 2021.

About half of all cyberattacks are committed against small businesses, says Steve Morgan, founder of Cybersecurity Ventures. He said the SHIELD Act will help raise cyber awareness among these firms.

"One primary reason small companies fall prey to cyber attacks is there isn't enough awareness," Morgan said.

The law includes guidance on administrative, technical and physical safeguards companies should follow when implementing or updating their data security programs, Breidenbach said. These include assessing and monitoring risks in network and software design; reasonable administrative safeguards include designating one or more employees to coordinate security; and physical safeguards include assessing risks of information storage and disposal.

There's a more flexible standard for small businesses with fewer than 50 employees that fall within a certain revenue/asset threshold. (For the full bill, see https://tinyurl.com/yexu4h7d.)

Those businesses "need to implement a reasonable security program appropriate for the size and complexity of their business," Rando-Copeland says.

These smaller firms could look for guidance from the Federal Trade Commission's cybersecurity best practices for small businesses (see https://tinyurl.com/yzhwsh8t), Breidenbach said.

"The New York attorney general when enforcing this law will likely look to the FTC's standards," he said. Potential civil penalties under the breach notification law have increased from $10 to $20 per instance of failed notification or $5,000, whichever is greater (capped at $250,000), Breidenbach said, and there are new civil penalties (up to $5,000 per violation, with no cap) for certain failures to comply with the new data security standards.

Firms may want to enlist professional tech guidance.

Benjamin Dynkin, co-founder of Great Neck-based Atlas Cybersecurity, says he performs an analysis at firms to identify security gaps and areas to strengthen.

He said even when companies think they have a handle on cybersecurity, they're often missing important elements.

"Sometimes it's policy updates and sometimes it's putting in certain basic controls like advanced malware protection," he says.

Dynkin said his firm has gotten some queries about SHIELD Act compliance, but expects more as the March deadline approaches. In January his company began new operations to monitor cyberactivity and threats for clients.

Zegers, of Ivionics Legal, said, "What it's forcing firms to do is look better at their data and manage their data better with more efficient practices."

COREY SIPKIN

Benjamin Dynkin, of Great Neck-based Atlas Cybersecurity, expects more inquiries about SHIELD Act compliance as the March deadline nears.

Company responsibilities after a breach

■ **Notify affected individuals** "in the most expedient time possible and without unreasonable delay" (unless there's a criminal investigation and then delay may be excusable under certain circumstances), Rando-Copeland says.

■ **Breach notices must include** (1) the contact information for the person or business making the notification; (2) the telephone numbers and websites of relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information; and (3) the categories of information and the elements of personal and private information that were or are reasonably believed to have been accessed/acquired, Breidenbach said.

■ **Related state legislation** signed the same day as the SHIELD Act requires a credit reporting agency that suffers a breach of information containing consumer Social Security numbers to provide five-year identity theft prevention services, and if applicable, identity theft mitigation services to affected customers.