P2JW142000-0-B00100-1--------XA

TECHNOLOGY: CHINA'S BAIDU DOES ABOUT-FACE ON PIRACY B4

BUSINESS & FINANCE

Last Week: S&P 2381.73 ▼0.38% S&P FIN ▼1.00% S&P IT ▼0.71% DJ TRANS ▼1.35% WSJ $ IDX ▼1.61% LIBOR 3M 1.186 NIKKEI 19590.76 ▼1.47% See more at WSJMarkets.com

Online Lenders Regain Footing

By Peter Rudegeair

The initial appeal of upstart online lenders was that they would disrupt traditional loan markets. But after big setbacks last year, the firms are adjusting to be a little more Wall Street and a little less Silicon Valley.

Changes include holding on to the risk of some loans they make, securitizing their loans—or selling them in packages—themselves rather than through third parties, and naming veterans of banks and investment firms to executive roles.

Investors in bonds backed by the loans these online platforms helped broker welcomed the moves. Last year, as skepticism mounted about their offerings, these investors pulled back from purchasing their loans. But since the start of April, more than $2 billion in securities backed by loans made by **LendingClub** Corp., **Prosper Marketplace** Inc. and their peers have either been sold or are being prepared for an imminent sale, according to credit-rating firms and people familiar with the matter. That is already more than was issued in the entire second quarter of 2016, according to data tracker PeerIQ.

Deals are also getting done at more favorable prices: The extra yield, or spread, investors demanded on recent deals from **Social Finance** Inc. and **Avant** Inc., above that of safe government debt, was much lower than on similar deals each lender brought last year.

The most recent activity comes on top of $3 billion in bonds backed by online loans that were issued in the first quarter of 2017, double the amount from the same period a year earlier, according to PeerIQ.

Early last year, confidence in these lenders was rocked by an upsurge in defaults, warnings from bond-rating firms and a scandal that forced out the CEO of industry leader LendingClub. Money managers responded by slowing their purchases of debt issued by these lenders and asked for higher yields.

Since then, online lenders have scrambled to make their credits more attractive to investors. They overhauled their lending criteria, cut off weaker consumers, shortened loan terms and started charging customers more to borrow in an attempt to boost yields.

"It was really important to see there was some kind of a consumer lending background...as opposed to just an algorithm," said Joe Astorina, head of asset-backed securities research at AllianceBernstein Holding LP.

Investors are embracing online lenders' debt offerings for their relative value compared with other debt, the better quality of underlying loans and moves they made to more closely resemble established finance firms rather than technology-driven startups.

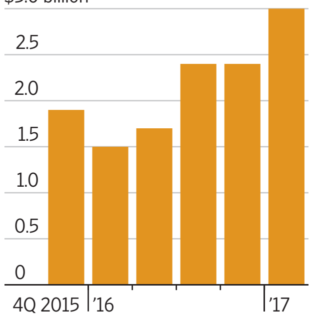
One factor working in lenders' favor: falling yields in other categories of debt, notably high-yield bonds. While yields on U.S. government debt rose following last November's election in anticipation of stronger economic growth, rates on high-yield debt fell due to expectations companies would fare better under the new administration. That made the lenders' loan packages more attractive on a comparative basis.

The spread demanded by money managers to hold

Please see LOANS page B2

Back in Demand

New issuance of bonds backed by loans from online lenders



Source: PeerIQ
THE WALL STREET JOURNAL.

Ford Weighs Executive Shake-Up

Ford Motor Co. is considering significant changes to the auto maker's senior leadership team amid tension among top executives, dissatisfaction with the stock price and a drive to clarify the company's strategy, according to people familiar with the situation.

By Christina Rogers, Joann S. Lublin and John D. Stoll

The moves could include a shuffling of executives who were hired or rose to prominence during the tenure of Alan Mulally, the company's chief executive for eight years ending in 2014. The current management team has been retooling the company to better prepare for shifts in the global auto industry.

A Ford spokesman declined to comment on management changes. The company is "staying focused on our plan for creating value and profitable growth," according to a statement.

Bill Ford, Ford's executive chairman, and the board are taking an influential role in the discussions, these people said. Mr. Ford served as CEO until Mr. Mulally's hiring. Chief Executive Mark Fields has proposed certain personnel changes as part of the process.

Mr. Fields has overseen a profitable three-year period at Ford as consumers have flocked to the pickup trucks and SUVs that the auto maker has long been known for. The lifetime Ford executive has routinely said he wants to transform the company's business model to better combat the threat presented by Silicon Valley tech firms, including Alphabet Inc., Apple Inc., Tesla Inc. and Uber Technologies Inc.

Mr. Fields's top lieutenants include Joe Hinrichs, the head of North American operations; and Jim Farley, who is credited with accelerating Ford's performance in Europe at a time when General Motors Co. is abandoning that region.

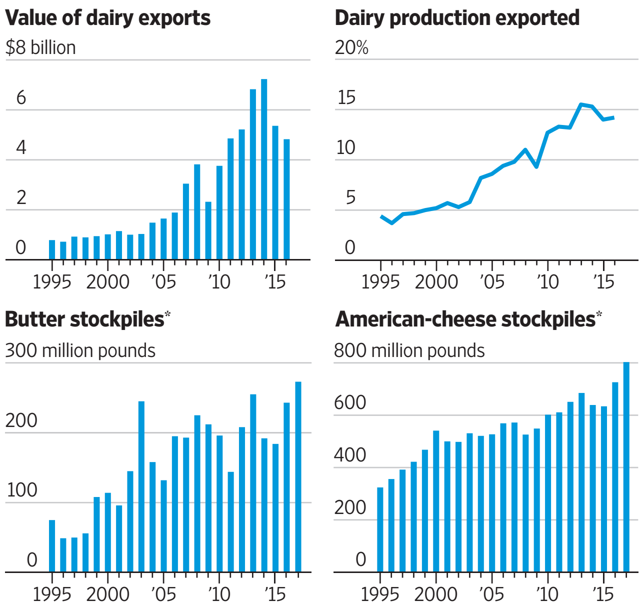
Last week, Ford granted retention bonuses to four senior executives including Mr. Farley, product chief Raj Nair and Hau Thai-Tang, head of purchasing. Messrs. Hinrichs and Fields weren't included in that series of grants.

Got Milk? Way Too Much, Say Farmers

Many bulked up their U.S. herds when prices were high, but then trouble in the global market hit

Creamed

U.S. dairy exports have declined amid growing product stockpiles.



*As of end-March
Sources: Agriculture Department; U.S. Dairy Export Council
THE WALL STREET JOURNAL.

DANIEL ACKER/BLOOMBERG

The U.S. dairy industry is taking a hit from weaker-than-expected demand and abundant supplies.

By Heather Haddon

U.S. dairy farmers' big bet on global demand for milk is souring.

The industry was in trouble long before a trade squabble with Canada last month that reduced demand for ultrafiltered milk, a cheese ingredient. Dairy farmers fear a spat that has jeopardized roughly $150 million in sales for Wisconsin, New York and Minnesota producers is just a prelude to disruptions to come if President Donald Trump renegotiates the North American Free Trade Agreement as promised.

"There was a perfect storm," said Jaime Castaneda, senior vice president of trade policy at the National Milk Producers Federation.

Dairy farmers aggressively expanded their herds three years ago when milk prices were driven up by growing demand from middle-class consumers in North America, Asia and other markets. By March, there were 9.4 million commercial dairy cows in the U.S., a 20-year high, according to the Agriculture Department.

But China, Russia, Venezuela and other importers scaled back their dairy purchasing in recent years due to domestic troubles. The European Union, meanwhile, greatly increased its dairy production after lifting 30-year-old quotas in 2015. Then came a world-wide surge in agricultural production that has pushed down prices for grains and meat as well as for dairy.

The dollar has also been on a multiyear climb, making U.S. exports less

Please see DAIRY page B2

ANDY MCMILLAN FOR THE WALL STREET JOURNAL

IT staffer Marty Norris, right, and program director Nathan Roland are seen at radio station WKSK.

KEYWORDS | By Christopher Mims

All IT Jobs Are Security Jobs Now

In the Appalachian mountain town of West Jefferson, N.C., on an otherwise typical Monday afternoon in September 2014, country radio station WKSK was kicked off the air by international hackers.

Just as the station rolled into its afternoon news broadcast, a staple for locals in this hamlet of about 1,300, a warning message popped up on the screen of the program director's Windows PC. His computer was locked and its files—including much of the music and advertisements the station aired—were being encrypted.

The attackers demanded $600 in ransom. If station officials waited, the price would double.

The station's part-time IT person, Marty Norris, was cruising in his truck when he got the call that something was amiss. He rushed to the station. "I immediately pulled the plug on his computer," says Mr. Norris.

In a quick huddle, the possibility of paying the ransom was raised, but the idea didn't get far. "We're a little bit stubborn in the mountains," says General Manager Jan Caddell. "It's kind of like being held up. We thought if we paid, they'd just ask for more."

Security experts believe this particular strain of ransomware has netted criminals

Please see MIMS page B4

The Fed Took a Road It Has Trouble Exiting

By Katy Burne

Federal Reserve officials grappling with the legacy of expansive stimulus would find it difficult to return to the central bank's precrisis role on the sidelines of financial markets, analysts and central-bank watchers say.

A long list of programs adopted to help foster economic growth, along with changes in money markets and bank regulation, have vastly expanded the Fed's balance sheet and its involvement in markets. The Fed's assets now total $4.5 trillion, up from less than $1 trillion a decade ago. Since 2013, the central bank has become one of the largest traders with U.S. taxable money-market funds, according to Crane Data.

Many analysts and investors worry that significantly rolling back the Fed's expansion, a course advocated by some in conservative circles, risks disrupting markets and the economy at a time when growth remains tepid. It would also reduce the connections the institution has built with a diverse set of Wall Street firms, beyond the group of banks it dealt with before the crisis.

The Fed has become "like an octopus," said Jeffrey Cleveland, chief economist at Payden & Rygel, a Los Angeles money manager. "Once you get the power and you are influencing all these markets, do you really want to retreat from all that?"

Investors are already assessing how stocks and bonds might react when the central bank begins the latest stage of its yearslong retreat from stimulus—likely later this year—by ending the practice of reinvesting the proceeds of maturing bonds into new bonds. The Fed is scheduled to publish Wednesday the minutes of its latest policy meeting, at which officials may have continued their debate over the mix of policy tools they plan to use in the future.

Some Fed officials say they are attracted to maintaining parts of their current approach. Minutes of their November meeting also showed officials discussing the advantages of keeping something similar to the existing system in place, in part because it is simpler to operate than the precrisis one.

The Fed hasn't decided the issue, but its choices will be closely watched because its leadership is in transition. President Donald Trump is preparing to fill three vacancies on the Fed's seven-member board. Republican lawmak-

Please see FED page B2

An About-Face for Baidu

Chinese search firm aggressively seeks to protect intellectual property it buys, creates

By Wayne Ma

NETFLIX/EVERETT COLLECTION

Baidu reached a deal with Netflix to air 'Stranger Things,' a scene from which is shown above.

BEIJING—Chinese search giant **Baidu** Inc. was once a scourge of Hollywood and the U.S. music industry, which accused it of being a pipeline for pirated content.

Today when Baidu is involved in a copyright infringement case, chances are it is the one casting the blame.

Baidu's about-face in the copyright fight reflects its emergence as a creator and buyer of content, a transition that continued recently when the company struck a deal to license original shows from **Netflix** Inc. Other Chinese media companies are undergoing similar transformations, upending how entertainment is protected in the world's second-largest economy, legal analysts say.

"One of the old rationales for copyright protection...is that it provides an incentive to invest. We are seeing that in play here in China," said Mathew Alderson, a partner and entertainment lawyer at Harris Bricken in Beijing. "Copyright is no longer something imposed on China by the U.S. It is now a tool in Chinese hands."

One way to measure the change is by the escalating flood of lawsuits aimed at protecting intellectual property.

Nearly 87,000 copyright-related cases were filed in China last year, according to data compiled by China's Supreme People's Court, a 15-fold increase from 2006. These cases include claims of illegal distribution, or unauthorized reproduction, of written content, videogames, movies and TV shows.

One of the companies filing suits is **iQiyi.com** Inc., the video-streaming service owned by Baidu that struck the April 25 deal with Netflix to bring shows such as the paranormal coming-of-age drama "Stranger Things" and the science-fiction series "Black Mirror" to the mainland.

Last year, iQiyi was the plaintiff in at least 133 copyright cases, up from 80 a year earlier, according to data provider IPHouse.

In addition to lawsuits, iQiyi sent takedown notices to more than 1,400 websites and apps last year—at one point sending more than 1,000 notices in a single day—to defend the licensed and original content it owns, according to Wang Yan, senior director of legal affairs at iQiyi.

Not that long ago, Baidu itself was the target of lawsuits by the music industry and Hollywood film studios for using content without permission.

"Baidu almost single-handedly eroded the value of music [in China]," said Neil Turkewitz, former vice president of international at the Recording Industry Association of America.

For nearly a decade, Mr. Turkewitz said, Baidu's search engine allowed users to find and play unlicensed songs directly from its web portal free.

The internet giant was sued in 2008 by major record labels **Warner Music Group**, **Universal Music** and **Sony BMG Music Entertainment** for violating music copyrights. At the time, the International Federation of Phonographic Industry estimated that record companies were receiving less than 5% of the estimated $700 million in potential annual revenue in China's mobile music space.

Baidu in 2011 announced it had struck a licensing deal with all three, effectively ending the lawsuit. That year, Baidu recorded its first line item for content costs: $9 million.

In 2013, Baidu was sued for violating video copyrights, this time by a group of Chinese entertainment companies supported by the Motion Picture Association and major Hollywood studios, which sought $43 million in damages.

The group accused Baidu of running four services on desktop computers and smartphones that they said allow users access to Western and Chinese TV shows and movies licensed to other companies. The plaintiffs added that in some instances, Baidu linked to sites that hosted pirated content.

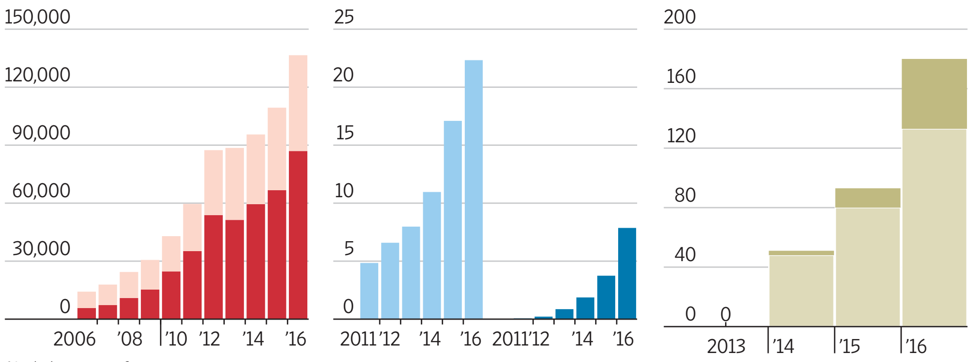
Baidu lost some of those lawsuits but ended up paying modest penalties.

A spokeswoman for Baidu declined to discuss how it has gone from being a defendant to a plaintiff in copyright cases.

Through its iQiyi streaming service, Baidu has become one of Hollywood's best customers, striking licensing deals with major studios such as **21st Century Fox**, **Warner Bros.** and **Paramount Pictures**.

China Gets Copyright Religion

China has seen an uptick in copyright cases in recent years, as Chinese firms defend the content and intellectual property they buy from others or create on their own.



*Includes agency fees

Sources: China's Supreme People's Court (cases); the companies; IPHouse (lawsuits)

THE WALL STREET JOURNAL.

SoftBank, Saudis Launch High-Tech Investment Fund

Japan's **SoftBank Group** and Saudi Arabia's sovereign-wealth fund on Saturday launched the world's largest technology fund, a nearly $100 billion vehicle that will steer capital to cutting-edge technologies in U.S. startups and other global firms.

By Margherita Stancati in Riyadh, Mayumi Negishi in Tokyo and Nicolas Parasie in Dubai

In a statement, SoftBank said the fund secured $93 billion of committed capital. The SoftBank Vision Fund is targeting a total of $100 billion within six months. The fund's creation coincides with U.S. President Donald Trump's two-day visit to Saudi Arabia, where he attempted to cement ties with a key counterterrorism ally and drum up business for American firms.

SoftBank Chief Executive Masayoshi Son has previously promised Mr. Trump that he would invest $50 billion of the fund in U.S. startups and create 50,000 jobs. Mr. Trump cited this as evidence of his presidency bringing jobs back home.

SoftBank said it would invest $28 billion in the fund, including $8.2 billion worth of its stake in chip architecture firm ARM Holdings Inc. SoftBank's announcement didn't specify the investment of its main partner, Saudi Arabia's **Public Investment Fund**. Earlier the PIF said it would invest as much as $45 billion in the fund.

"We can make a lot of new initiatives and make entrepreneurs take off a lot quicker, much bigger," Mr. Son said Saturday on the sidelines of a business forum in Riyadh.

Mr. Son is rushing to invest in key technologies ahead of what he predicts will be a robotic revolution and a rush of investment into areas such as deep learning and robotics. The fund enables SoftBank to invest in emerging technologies as artificial intelligence surpasses human capabilities.

The fund is looking to acquire minority and majority interests in private and public companies, according to a statement. It would consider not only emerging technology businesses but also more established, multibillion-dollar companies requiring substantial funding, it said.

SoftBank has negotiated about a dozen deals for the fund, among them deals to invest $1.4 billion in Indian mobile-payments startup Paytm and $1.2 billion in U.S. satellite-internet startup OneWeb Ltd. SoftBank also has led a $502 million fundraising in U.K. virtual-world startup Improbable and an additional $130 million fundraising in Bay Area microbe-designing robot firm Zymergen. All investments of more than $100 million, with the exception of those in ride-hailing firms, will go to the fund, people familiar with the matter have said.

Ahead of the fund's launch on Saturday, Mr. Son said it would focus on investing in sectors including artificial intelligence, smart devices and semiconductors. "We already have lots in the pipeline," he said. "We are investing into genome sequencing. We are investing in virtual-reality simulations, the games, and so on."

$93B

Capital committed to SoftBank Vision Fund

The fund marks the entry of a mammoth player in a field of investment traditionally dominated by Western bankers and private-equity groups. The sheer scale of the fund could decide winners and losers in capital-intensive areas, such as in autonomous driving or in biotechnology.

It also follows months of negotiation and delay as SoftBank and Saudi Arabia's PIF wrangled over who would control investment decisions. Mr. Son announced the fund in October with a launch as early as December in mind. It took a further five months for the fund to come together.

MIMS

Continued from page B1

at least $325 million in extorted payments so far, but the real figure could easily be twice that.

The global "WannaCry" ransomware attack that peaked last week, and has affected at least 200,000 computers in 150 countries, as well as the growing threat of Adylkuzz, another new piece of malware, illustrate a basic problem that will only become more pressing as ever more of our systems become connected: The internet wasn't designed with security in mind, and dealing with that reality isn't cheap or easy.

Despite all the money spent—Gartner estimates $81.6 billion on cybersecurity in 2016—things are, on the whole, getting worse, says Chris Bronk, associate director of the Center for Information Security Research and Education at the University of Houston. "Some individual companies are doing better," adds Dr. Bronk. "But as an entire society, we're not doing better yet."

Ever greater profits from cyberattacks mean cybercriminals have professionalized to the point that they are effectively criminal corporations, says Matthew Gardiner, a cybersecurity strategist for Mimecast, which manages businesses' email in the cloud. Instead of hackers fumbling their way through complicated financial transactions or money wizards fumbling their way through malware design, there is true division of labor. As in any other industry, specialization begets efficiency.

Large (legitimate) corporations have the resources to hire talent to protect their digital assets, but for small- and medium-size businesses, it is harder. There is no shortage of good advice on how to perform basic security hygiene, but who is there to implement it? The solution is resource management, with a focus on cybersecurity. Dr. Bronk lays it out like this:

1. Retrain IT staff on security—or replace them. In today's world of ever-multiplying threats and dependence on connected assets, all IT staff must now be cybersecurity staff first. "The good news is that you don't need that dedicated person to run your email server anymore—they can run security," says Dr. Bronk.

2. Push everything to the cloud. It used to be the job of IT personnel was to build and maintain the tools employees need. Now, pretty much anything can be done better with a cloud-based service. "I mean, even the CIA uses Amazon's web services," says Dr. Bronk. "If there's a best of breed, why not use it? If you want a safe car, go buy a Volvo."

3. New IT investment will need baked-in security. Data from the Bureau of Labor Statistics indicate jobs in IT security are one of the fastest-growing categories in tech, up 33% in the past four years alone. That is probably due to companies simply catching up on investing in cybersecurity after years of underinvestment, says Mr. Gardiner.

Diana Kelley, global executive security adviser at IBM Security, a division of International Business Machines Corp., compares the current state of network security to graphical user interfaces in their earliest days, when they weren't particularly intuitive. Collectively, designers and engineers learned to prioritize and improve them. "Security can be like that, too," she adds. "We can think about it upfront and weave it into the process in a much more effective way."

The cloud isn't perfect, of course. A hack of electronic-signature company **DocuSign**, disclosed last week, exposed customer email addresses, allowing attackers to target them with convincing emails that included a malware attachment disguised as a Microsoft Word doc. And then there is the fact that massive denial-of-service attacks like Mirai can make the cloud inaccessible at critical times.

WannaCry is a good example of how increasing cybersecurity can be relatively simple—thwarting it was as simple as keeping Windows up to date. On the other hand, it used a sophisticated exploit lifted from a hack of National Security Agency tools that allowed it to spread directly from one computer to another, infecting systems in companies that might have been prepared for other kinds of attacks.

These kinds of systemic weaknesses employed by or stolen from governments have led Microsoft to plead for a "Geneva Convention" on cyberweapons.

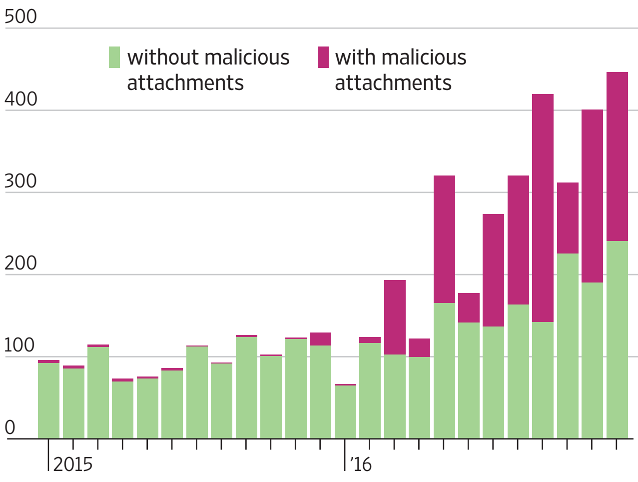
As for West Jefferson's own WKSK, the station was lucky: Mr. Norris, its IT consultant, had backed up the computers. He was able to wipe the slate clean and get everyone back on the air in a few hours. It is a good illustration of how prioritizing even the most basic cybersecurity practices can be a life-saver.

Since then, he has implemented offline backups of the station's computers, just in case. He also has become a keen student of the kind of attacks, such as WannaCry, that can affect small organizations. As soon as he read that it could hit older systems, he rushed to protect them at his day job—as the IT person for the local school district.

Don't Open That Attachment

The past year has seen a meteoric increase in emails around the globe containing malware, according to a recent IBM Security study.

Change in amount and type of spam email, 1Q 2015 = 100

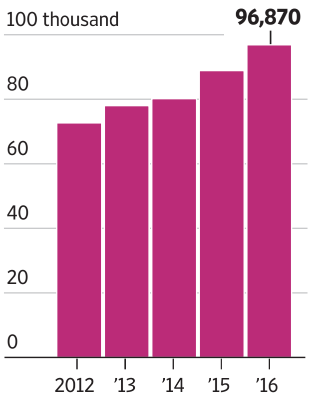


Source: IBM X-Force

THE WALL STREET JOURNAL.

Cybersecurity Guards

Total U.S. employment of information security analysts



Source: Bureau of Labor Statistics

THE WALL STREET JOURNAL.