F-Secure Corporation

U.S. POST OFFICE
DELAYED

82-5035

December 20, 2001

RE: Rule 12g3-2(b) submission by F-Secure Corporation (formerly, Data Fellows Corp.)

Securities and Exchange Commission
Judiciary Plaza
450 Fifth Street, N.W.
Washington, D.C. 20549
USA

SUPPL

Attention: Division of International Corporate Finance

Ladies and Gentlemen:

I refer to the above-referenced exemption pursuant to Rule 12g3-2(b) (the "Rule") under the Securities Exchange Act of 1934, as amended (the "Act"), granted previously to F-Secure Corporation (formerly Data Fellows Corp.). I hereby transmit to you, in accordance with the provisions of Rule 12g3-2(b)(4) of the Act, a recent press release published by F-Secure.

As stated in paragraph (5) of the Rule, the Company understands that its furnishing the Securities and Exchange Commission with the information set forth above and the documents being transmitted herewith pursuant to the Rule shall not constitute an admission for any purpose that the Company is subject to the provisions of the Act.

Please contact the undersigned in connection with any of the points discussed in this letter.

Very truly yours,

dlw 2/7

Jaana Sirkiä
Corporate communicator

P. Henrietta Malmari

Press release

F-Secure Corporation
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
http://www.F-Secure.com

FOR RELEASE December 18, 2001

2001: A Security Odyssey

F-Secure recalls the most challenging year for data security ever

Helsinki, December 18, 2001 - Experts agree that year 2001 was the most active year for computer related crime so far. The year 2001 was, to paraphrase Arthur C. Clarke, a security odyssey, said Mikko Hypponen, Manager of Anti-Virus Research at F-Secure Corporation.

From traditional viruses to complex network worms

One of the central themes of 2001 was the rapid evolution of the malicious code threat. Many of the new computer virus types we saw during 2001 were using hacking techniques such as exploiting known security vulnerabilities.Worms such as Code Red are difficult to stop with traditional anti-virus solutions, because they never infect files."To combat these new types of combined hacking and virus attacks the data security industry needs to combine functionality from traditional anti-virus programs and distributed firewall systems, providing protection against viruses, hacking and the combination of these", says Hypponen. A state of dread among savvy and novice computer users alike, first perceived in the year 2000, was amplified in 2001. Viruses continued to appear at the rate of five per day, according to Hypponen, and by year-end had accumulated to 59,000.

Nimda worm

Perhaps most notorious for its damage and for what it portends was the mass-mailing Nimda worm, the first Internet malware that actually took over websites in order to proliferate. Spread by four different methods, Nimda infected 2.5 million computers, taking just one day to infect local area networks and individual desktops globally. "We have no idea where Nimda came from. There are references to China inside, but those could be faked", comments Hypponen. Wherever it's from, it's likely to be written by a group of people. And to develop and test a worm like Nimda, a testing lab with networks, servers and routers is needed. The size of the investment in both time and money makes one wonder what are the motives driving the creators of viruses like Nimda.

Much of the damage done by Nimda and a later worm called BadTrans was avoidable, in that preventive measures were freely available. In addition to commercial anti-virus products, Microsoft had warned of certain vulnerabilities in its applications, and offered a free patch; but many users were lax in a false sense of security and did not update their

systems. "That's skating on very thin ice", said Hypponen, "and many fell through".

But the world of anti-virus research wasn't without its victories either; both the Dutch author of Anna Kournikova virus and a group of Israelian teenagers behind the Goner virus were located and apprehended by authorities. "The only way we can win is by getting these vigilantes caught and showing the world virus-writing is a crime which doesn't pay", comments Hypponen.

An example of devious craft showed itself in the distribution of viruses and other malware through mailing-list servers. Most members of affinity groups, such as music fan clubs and other opt-in organizations, open the email from those servers because, either consciously or instinctively, they trust the content. In just the first month of testing protective software provided by F-Secure, L-Soft reported stopping more than 100,000 virus attacks on some 630 lists hosted by that company.

Although most of the security problems over 2001 concerned users of Microsoft operating systems, other platforms had their share as well: In January, the first widespread Linux worm, known as Ramen, was found. In May, the Sadmind worm infected hundreds of Solaris-based Unix systems. And in June, Macintosh users had their share of e-mail mass mailing worms with the discovery of the Mac.Simpsons worm.

What lies ahead

Meanwhile, a wave of enthusiasm greeted Nokia's new smart phones and Microsoft's latest PDA platform, Pocket PC 2002. With the proliferation of mobile devices across enterprises, corporate assets ranging from e-mail to confidential financial information instantly become more vulnerable to theft or damage. Pocket PC 2002 and Nokia Communicator herald a whole new generation of wireless devices, many in the hands of end-users, with all the exposure and vulnerability that comes with the territory of such new products.

"The security risks that these present to businesses will multiply in January, as many professionals will bring the PDAs they have received as Christmas gifts into work, and start to place corporate data on them.This data is then at risk of interception, loss, theft and worse, underlining the need for IT managers to have solutions which cover the entire IT spectrum with strong encryption and content (anti-virus) security", said Anthony Gyursanszky, Vice President, Wireless Security Solution Unit of F-Secure Corporation.

Unfortunately, the future looks no brighter, says Hypponen. Human tendencies persist. And, those who get some diabolical pleasure out of attacking technology continue their destruction at an accelerating pace. In anticipation of continuing activity on this front, F-Secure increased its anti-virus signature updates to twice daily, which is believed to be the most frequent updating in the industry. It is sensible to assume that the number of sophisticated malicious code attacks will increase. The attacks are getting more and more professional.Whether these people represent terrorist groups, organized crime, military or intelligence communities is somewhat irrelevant. The bottom line is that we are seeing the first signs of the type of fundamental vulnerability that a fully computerized society and economy will have to live with.

F-Secure Corporation • PL 24, FIN-00181 Helsinki, FINLAND • tel. +358 9 2520 0700, fax +358 9 2520 5001

Appendix: Major virus cases of 2001

January: Hybris January: Matrix (MTX) February: Anna Kournikova March: Magistr May: Homepage July: Sircam July: Code Red September: Nimda November: Badtrans December: Goner

Descriptions and screenshots of the above viruses are available from http://www.f-secure.com/v-descs/

About F-Secure Corporation

F-Secure Corporation is a leading provider of centrally managed security for today's mobile, wireless enterprise. The company offers a full range of award-winning, integrated anti-virus, file encryption, distributed firewall and VPN solutions for workstations, servers, gateways and mobile devices. F-Secure products are uniquely suited for delivery of Security as a Service (TM) which provides invisible, reliable, always-on, and up-to-date security for the most widely distributed user base. Whether provided by corporate IT or delivered by service providers, F-Secure solutions extend policy-based security and instant alerts to all devices where information is created, stored or accessed. Founded in 1988, F-Secure Corporation is listed on the Helsinki Stock Exchange [HEX: FSC]. The company is headquartered in Espoo, Finland with North American head office in San Jose, California, as well as offices worldwide.

For more information, please contact:

F-Secure Corporation
Mikko Hypponen, Manager, Anti-Virus Research
PL 24
FIN-00181 Helsinki
Tel. +358 9 2520 5513
Fax +358 9 2520 5001
Mobile: +358 400 648 180
Email: Mikko.Hypponen@F-Secure.com